

**UNIVERSIDADE REGIONAL DO NOROESTE DO ESTADO DO RIO
GRANDE DO SUL
DEPARTAMENTO DE MATEMÁTICA, FÍSICA E ESTATÍSTICA
CURSO DE MESTRADO EM MODELAGEM MATEMÁTICA**

**SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS COM
APLICAÇÃO EM COMUNICAÇÃO SEGURA**

DISSERTAÇÃO DE MESTRADO

José Mario Vicensi Grzybowski

Ijuí, RS, Brasil.

2008

Livros Grátis

<http://www.livrosgratis.com.br>

Milhares de livros grátis para download.

SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS COM APLICAÇÃO EM COMUNICAÇÃO SEGURA

Por

José Mario Vicensi Grzybowski

Dissertação apresentada ao Curso de Mestrado em Modelagem Matemática do
Departamento de Física, Estatística e Matemática e do Departamento de
Tecnologia da Universidade Regional do Noroeste do Estado do Rio Grande do Sul
(UNIJUÍ), como requisito parcial para obtenção do grau de
Mestre em Modelagem Matemática

Orientador: Prof. Dr. Marat Rafikov

Ijuí, RS, Brasil.

2008

**UNIVERSIDADE REGIONAL DO NOROESTE O ESTADO DO RIO
GRANDE DO SUL
PROGRAMA DE PÓS-GRADUAÇÃO EM MODELAGEM
MATEMÁTICA**

A Comissão Examinadora, abaixo assinada, aprova a Dissertação

**“SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS COM APLICAÇÃO
EM COMUNICAÇÃO SEGURA”**

Elaborada por

JOSÉ MARIO VICENSI GRZYBOWSKI

Como requisito para a obtenção do grau de Mestre em Modelagem Matemática

Comissão Examinadora

Prof. Dr. Marat Rafikov – (Orientador) UNIJUI

Prof. Dr. Rosemaira Dalcin Copetti - UFSM

Prof. Dr. Antonio Carlos Valdiero – UNIJUI

Ijuí-RS, 10 de março de 2008.

“Ou a vida é uma aventura ousada ou é nada.”

Helen Keller

*“Porque a forma de todo o universo é a mais perfeita e,
de fato, projetada pelo mais sábio Criador,
nada em todo este mundo ocorrerá
sem que o brilho de uma regra
de máximo ou mínimo
esteja presente.”*

Leonhard Euler

Agradeço aos meus pais (*in memorian*),
pela vida, pelo amor e pela oportunidade;
à minha família e amigos, pelo incentivo;
ao mestre Marat, pela atenção, paciência
e por compartilhar sua sabedoria,
bom-humor e piadas sobre gremistas;
aos colegas e seus formidáveis estômagos,
pela convivência, pela partilha
e pela companhia em tantas pizzas.

RESUMO

O presente trabalho estuda a dinâmica dos sistemas caóticos e metodologias de controle e sincronização de caos, em especial o controle ótimo linear feedback para sistemas não-lineares com uma aplicação para a sincronização de caos em sistemas de comunicação segura. O problema do controle ótimo linear feedback para sistemas não-lineares é formulado, resolvido e, a seguir, aplicado em um algoritmo criptográfico baseado em sincronização de caos. O funcionamento do algoritmo é simulado numericamente e a seguir avaliado nos aspectos segurança, desempenho e custo computacional.

Palavras-chave: caos, controle ótimo, sincronização, comunicação segura.

ABSTRACT

This paper studies chaotic dynamics and methodologies for chaos control and synchronization, specially the optimal linear feedback control for nonlinear systems methodology, as well as an application of chaos synchronization in secure communication systems. The optimal linear feedback control for nonlinear systems problem is formulated, solved and applied in an cryptographic algorithm based in chaos synchronization. The algorithm is numerically simulated and evaluated in aspects such as security, performance and computational effort.

Keywords: chaos, optimal control, synchronization, secure communication.

LISTA DE FIGURAS

<i>Figura 1 - Biliar de Sinai com condições iniciais minimamente diferentes</i>	<i>15</i>
<i>Figura 2 - Esquema da célula de Rayleigh-Bénard</i>	<i>21</i>
<i>Figura 3 - Atrator de Lorenz.....</i>	<i>22</i>
<i>Figura 4 - Expoentes de Lyapunov do sistema de Lorenz.....</i>	<i>25</i>
<i>Figura 5 - Dinâmica dos expoentes de Lyapunov – Sistema de Lorenz.....</i>	<i>26</i>
<i>Figura 6 - Dinâmica dos expoentes de Lyapunov (zoom em λ_1 e λ_2) – Sistema de Lorenz.....</i>	<i>26</i>
<i>Figura 7 - Seção de Poincaré do sistema de Lorenz.....</i>	<i>27</i>
<i>Figura 8 - Mapa de Poincaré do sistema de Lorenz, $x_1=1$.....</i>	<i>27</i>
<i>Figura 9 - Atrator de Chen.....</i>	<i>28</i>
<i>Figura 10 - Expoentes de Lyapunov para o sistema de Chen</i>	<i>31</i>
<i>Figura 11 - Dinâmica dos expoentes de Lyapunov</i>	<i>32</i>
<i>Figura 12 - Dinâmica dos expoentes de Lyapunov (zoom em λ_1 e λ_2).....</i>	<i>32</i>
<i>Figura 13 - Seção de Poincaré do sistema de Chen.....</i>	<i>33</i>
<i>Figura 14 - Mapa de Poincaré do sistema de Chen, $x_1=1$</i>	<i>33</i>
<i>Figura 15 - Atrator de Lü.....</i>	<i>34</i>
<i>Figura 16 - Expoentes de Lyapunov do sistema de Lü.....</i>	<i>37</i>
<i>Figura 17 - Dinâmica dos expoentes de Lyapunov</i>	<i>38</i>
<i>Figura 18 - Dinâmica dos expoentes de Lyapunov (zoom em λ_1 e λ_2).....</i>	<i>38</i>
<i>Figura 19 - Seção de Poincaré do sistema de Lü.....</i>	<i>39</i>
<i>Figura 20 - Mapa de Poincaré do sistema de Lü, $x_1=1$</i>	<i>39</i>
<i>Figura 21 - Atrator de Lorenz, $\alpha=0$.....</i>	<i>40</i>
<i>Figura 22 – Atrator de Lü, $\alpha=0,8$.....</i>	<i>41</i>
<i>Figura 23 - Atrator de Chen, $\alpha=1$.....</i>	<i>41</i>
<i>Figura 24 - Expoentes de Lyapunov - sistema caótico unificado.....</i>	<i>42</i>
<i>Figura 25 - Erro de sincronização dos sistemas de Lorenz acoplados.....</i>	<i>49</i>
<i>Figura 26 - Erro de sincronização dos sistemas de Lorenz com observador.....</i>	<i>51</i>
<i>Figura 27 - Erro de sincronização dos sistemas de Lorenz com Controle mestre-escravo</i>	<i>53</i>
<i>Figura 28 - Erro de sincronização do sistema de Lorenz via controle não-linear.....</i>	<i>55</i>
<i>Figura 29 - Erro de sincronização sistemas de Chen e Lorenz - controle ativo</i>	<i>58</i>
<i>Figura 30 - Dinâmica dos sistemas de Lorenz em 2D.....</i>	<i>67</i>
<i>Figura 31 - Erro de sincronização - Sistema de Lorenz.....</i>	<i>67</i>
<i>Figura 32 - Avaliação da função $l(x,e)$ – Sistema de Lorenz</i>	<i>68</i>
<i>Figura 33 - Dinâmica dos sistemas de Chen em 2D</i>	<i>69</i>
<i>Figura 34 - Erro de sincronização - Sistema de Chen</i>	<i>69</i>
<i>Figura 35 - Avaliação da função $l(x,e)$ - Sistema de Chen.....</i>	<i>70</i>
<i>Figura 36 - Dinâmica dos sistemas de Lü em 2D.....</i>	<i>71</i>
<i>Figura 37 - Erro de sincronização - Sistema de Lü</i>	<i>71</i>
<i>Figura 38 - Avaliação da função $l(x,e)$ – Sistema de Lü.....</i>	<i>72</i>
<i>Figura 39 - Sincronização do sistema caótico unificado com controle escalar.....</i>	<i>74</i>
<i>Figura 40 - Erro de sincronização – controle escalar</i>	<i>74</i>
<i>Figura 41 - Sincronização do sistema caótico unificado com controle vetorial</i>	<i>75</i>
<i>Figura 42 - Erro de sincronização – controle vetorial</i>	<i>76</i>
<i>Figura 43 - Tempo e custo da sincronização - sistema de Lorenz, $q_{ii}=10$ a $q_{ii}=100$</i>	<i>81</i>
<i>Figura 44 - Tempo e custo da sincronização - sistema de Lorenz, $q_{ii}=100$ a $q_{ii}=1000$</i>	<i>81</i>
<i>Figura 45 - Tempo e custo da sincronização - sistema de Lorenz, $q_{ii}=1000$ a $q_{ii}=10000$</i>	<i>82</i>
<i>Figura 46 - Tempo e custo da sincronização - sistema de Chen, $q_{ii}=10$ a $q_{ii}=100$.....</i>	<i>82</i>
<i>Figura 47 - Tempo e custo da sincronização - sistema de Chen, $q_{ii}=100$ a $q_{ii}=1000$.....</i>	<i>83</i>
<i>Figura 48 - Tempo e custo da sincronização - sistema de Chen, $q_{ii}=1000$ a $q_{ii}=10000$.....</i>	<i>83</i>
<i>Figura 49 - Tempo e custo da sincronização - sistema de Lü, $q_{ii}=10$ a $q_{ii}=100$.....</i>	<i>84</i>
<i>Figura 50 - Tempo e custo da sincronização - sistema de Lü, $q_{ii}=100$ a $q_{ii}=1000$.....</i>	<i>84</i>
<i>Figura 51 - Tempo e custo da sincronização - sistema de Lü, $q_{ii}=1000$ a $q_{ii}=10000$.....</i>	<i>85</i>
<i>Figura 52 - Sincronização do sistema de Lorenz via controle contínuo por partes, $\varepsilon=0,02$.....</i>	<i>91</i>
<i>Figura 53 – Erro de sincronização do sistema de Lorenz via controle contínuo por partes, $\varepsilon=0,02$</i>	<i>91</i>

<i>Figura 54 - Avaliação da função $l(x,e)$ na trajetória, $\varepsilon=0,02$.....</i>	<i>92</i>
<i>Figura 55 - Sincronização sistema de Lorenz via controle contínuo por partes, $\varepsilon=0,01$.....</i>	<i>93</i>
<i>Figura 56 - Erro de sincronização sistema de Lorenz via controle contínuo por partes, $\varepsilon=0,01$.....</i>	<i>93</i>
<i>Figura 57 - Avaliação da função $l(x,e)$ na trajetória, $\varepsilon=0,01$.....</i>	<i>94</i>
<i>Figura 58 - Tempo aproximado de atuação do controle em relação ao.....</i>	<i>94</i>
<i>Figura 59 - Máscara caótica aditiva.....</i>	<i>102</i>
<i>Figura 60 - Modulação caótica.....</i>	<i>103</i>
<i>Figura 61 - Criptossistema caótico.....</i>	<i>103</i>
<i>Figura 62 - Imagem original.....</i>	<i>106</i>
<i>Figura 63 - Imagem encriptada.....</i>	<i>106</i>
<i>Figura 64 - Imagem recuperada.....</i>	<i>107</i>
<i>Figura 65 - Esquema de funcionamento do algoritmo.....</i>	<i>110</i>
<i>Figura 66 - Lenna Picture original (tons de cinza).....</i>	<i>112</i>
<i>Figura 67 - Lenna picture encriptada (tons de cinza).....</i>	<i>112</i>
<i>Figura 68 - Lenna Picture recuperada (tons de cinza).....</i>	<i>113</i>
<i>Figura 69 - Lenna Picture original (padrão RGB).....</i>	<i>113</i>
<i>Figura 70 - Lenna Picture encriptada (padrão RGB).....</i>	<i>114</i>
<i>Figura 71 - Lenna Picture recuperada (padrão RGB).....</i>	<i>114</i>
<i>Figura 72 - Tentativa de decriptação utilizando chave incorreta.....</i>	<i>115</i>

SUMÁRIO

<i>INTRODUÇÃO</i>	1
<i>1 SISTEMAS DINÂMICOS CONTÍNUOS E CAOS</i>	5
1.1 Introdução	5
1.2 A descoberta do Caos.....	5
1.3 Sistemas dinâmicos contínuos, pontos fixos e estabilidade	7
1.4 Expoentes característicos de Lyapunov	12
1.5 Dissipatividade e o divergente.....	14
1.6 Atratores Estranhos.....	14
1.7 Mapas e Seção de Poincaré	16
1.8 Caracterização do caos determinístico.....	16
1.9 Considerações finais	18
<i>2 ESTUDO DOS MODELOS MATEMÁTICOS</i>	20
2.1 Introdução	20
2.2 Sistema de Lorenz.....	20
2.3 Sistema de Chen	27
2.4 Sistema de Lü	33
2.5 Sistema caótico unificado	39
2.6 Considerações finais	42
<i>3 SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS</i>	43
3.1 Introdução	43
3.2 Sincronização na natureza	44
3.3 Sincronização de caos	45
3.4 Alguns enfoques da sincronização de caos.....	46
3.5 Considerações finais	58
<i>4 SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS VIA CONTROLE ÓTIMO LINEAR FEEDBACK</i>	60
4.1 Introdução	60
4.2 Regulador ótimo linear com funcional quadrático	61
4.3 Sincronização de sistemas não-lineares via controle ótimo linear feedback	62
4.4 Simulações numéricas.....	65

4.5 Considerações finais	76
5 SELEÇÃO DA MEDIDA DE DESEMPENHO: AVALIAÇÃO DE CUSTO E TEMPO NECESSÁRIO PARA SINCRONIZAÇÃO.....	78
5.1 Introdução	78
5.2 Seleção da medida de desempenho	79
5.3 Simulações numéricas.....	80
5.4 Considerações finais	86
6 SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS VIA CONTROLE LINEAR FEEDBACK CONTÍNUO POR PARTES	88
6.1 Introdução	88
6.2 O controle linear feedback contínuo por partes.....	88
6.3 Simulações Numéricas.....	90
6.4 Considerações finais	94
7 SINCRONIZAÇÃO DE CAOS APLICADA À COMUNICAÇÃO SEGURA.....	96
7.1 Introdução	96
7.2 Princípios básicos da comunicação segura	97
7.3 Comunicação segura baseada em caos.....	101
7.4 Estudo de um algoritmo de encriptação baseado em caos	104
7.5 Considerações finais	107
8 PROPOSTA DE UM ALGORITMO DE ENCRIPTAÇÃO BASEADO EM SINCRONIZAÇÃO DE CAOS	109
8.1 Introdução	109
8.2 Algoritmo de encriptação baseado em sincronização de caos.....	110
8.3 Simulações numéricas.....	112
8.4 Considerações finais	115
CONCLUSÕES.....	117
REFERÊNCIAS.....	120
APÊNDICE A: CRITÉRIO DE ROUTH-HURWITZ.....	127
APÊNDICE B: SKEW TENT MAP	128

INTRODUÇÃO

Nos últimos anos, um número crescente de pesquisadores e instituições têm dedicado seu tempo ao estudo dos fenômenos não-lineares. Depois de muitas décadas dedicadas às simplificações e busca de explicações em modelos lineares, a ciência volta-se com muita força para o estudo e compreensão do não-linear, em especial do caos.

Sistemas caóticos despertam grande fascinação porque encerram, mesmo em equações simples, um comportamento rico, complexo e exuberante. A impossibilidade prática de efetuar previsões acerca do comportamento desse tipo de sistema determinístico, resultado do “efeito borboleta” ou “sensibilidade às condições iniciais”, é característica dos sistemas que exibem caos. A sensibilidade às condições iniciais significa que sistemas caóticos amplificam exponencialmente quaisquer incertezas em suas condições iniciais de forma que, após um período arbitrário de tempo, a incerteza do estado de um sistema caótico será da ordem da própria amplitude do movimento [54].

Dentro da novíssima ciência do caos, a sincronização tem atraído muita atenção por se tratar de uma área promissora com campo excepcionalmente multidisciplinar. Entre os mais notórios campos de aplicação da sincronização encontram-se a engenharia elétrica e a medicina.

De uma forma geral, a sincronização de osciladores pode ocorrer de maneira espontânea ou induzida. A sincronização espontânea ocorre em sistemas naturais acoplados quando, por exemplo, milhões de neurônios disparam ao mesmo tempo para controlar a respiração e os batimentos cardíacos. A sincronização induzida, por sua vez, utiliza-se de mecanismos de controle para induzir dois ou mais osciladores a atingirem sincronização. Sistemas de encriptação, por exemplo, requerem um mecanismo de sincronização para certificar-se de que o bit correto está sendo decodificado no tempo correto [71].

Na engenharia elétrica a sincronização sempre teve papel fundamental, visto que todas as aplicações de comunicação sem fio baseiam-se em sincronização. Nesse contexto, a sincronização de caos é promissora porque tem potencial para agregar segurança a tais aplicações e oferecer sigilo e privacidade num mundo de comunicação instantânea. Os sinais determinísticos, pseudo-aleatórios e sensíveis a perturbações,

gerados pelos sistemas caóticos, são indesejáveis em áreas tais como a engenharia mecânica e medicina, ao mesmo tempo em que são fundamentais em se tratando da aplicação em comunicação segura na forma como tem sido proposta na literatura especializada recente.

De uma maneira geral, sistemas caóticos possuem comportamento altamente complexo e organizado e possuem características análogas às desejáveis em métodos consagrados da criptografia clássica. Assim, ao mesmo tempo em que é uma característica indesejável nas mais diversas aplicações, essa incerteza cumpre papel fundamental em se tratando da aplicação em comunicação segura¹.

Mas, qual é afinal a potencial vantagem da comunicação segura baseada em caos sobre a criptografia clássica? A possibilidade de implementação de sistemas caóticos em *hardware* [80] pode permitir que o custo computacional da encriptação e decriptação sejam consideravelmente reduzidos. Essa sempre foi uma das maiores preocupações da criptografia clássica, pois seria possível atingir um nível de segurança altíssimo se tivéssemos à disposição uma capacidade de processamento infinito. Assim, como na prática a capacidade de processamento é um dos fatores limitantes da segurança de um algoritmo, a implementação da comunicação baseada em caos poderia, em parte, resolver esse problema, além de tornar a encriptação/decriptação mais ágil e veloz.

Assim, diversos trabalhos têm se dedicado a propor sistemas criptográficos baseados em sincronização de sistemas caóticos e a enfrentar uma das três dificuldades principais com que a técnica se depara: a sincronização, que é a base sobre a qual todo o processo criptográfico é desenvolvido; o ruído, que é um fator limitante, de forma especial no caso de sinais analógicos; e a segurança, que é o objetivo final dos algoritmos.

Algumas características desejáveis dos algoritmos criptográficos baseados em caos, como a facilidade de implementação e custo aceitável, geralmente não são mencionadas pois constituem-se em condições básicas para a aplicabilidade de tais algoritmos.

Neste trabalho enfocaremos exclusivamente o problema da sincronização, através da apresentação e aplicação da metodologia do controle ótimo linear feedback a sistemas não-lineares, conforme proposta em [64].

¹ Refere-se à condição de que uma informação possa ser transmitida a determinado destinatário através de um canal público sem que outras pessoas possam tomar conhecimento de seu conteúdo.

No contexto dos sistemas e algoritmos de comunicação baseados em caos, a aplicação pode ser projetada para funcionar com sinais analógicos ou sinais digitais e, alternativamente, para a comunicação baseada em computadores, através de FPGA² [68]. No presente trabalho, dedicaremos nossa atenção aos sistemas de comunicação analógica baseados em caos.

Diversos trabalhos propuseram diferentes metodologias para controle e sincronização de caos. Em primeiro lugar merecem menção os trabalhos pioneiros de Pecora e Carroll [59, 60] e de Ott, Grebogi e Yorke [32]. A partir dessas publicações, muitas outras foram dedicadas ao problema, utilizando diferentes enfoques, métodos e técnicas: [35, 52, 75] propõem o uso de controle *backstepping* não-linear recursivo para sistemas caóticos do tipo *jerk*³; [16, 30, 31, 61] utilizam metodologias de projeto de sistemas observadores globalmente estáveis; [27, 45] utilizam o acoplamento linear unidirecional e bidirecional; [24, 25] fazem uso de controle não-linear; [9, 34, 36, 37, 64, 65] utilizam a metodologia de controladores lineares com realimentação; [72, 79] utilizam controle ativo; [63] propõe a utilização de controle ótimo para controlar o sistema de Rössler e, finalmente [47, 53, 77] utilizam controle adaptativo, para citar alguns.

Neste trabalho apresentamos um breve estudo de três sistemas caóticos (sistemas de Lorenz, Chen e Lü) e de seis enfoques diferentes com que a sincronização de caos pode ser abordada. Por fim, apresentamos um algoritmo para comunicação baseada em caos e simulações numéricas com resultados de sua aplicação.

De uma forma geral, os objetivos desse trabalho são:

- estudar a dinâmica dos sistemas caóticos;
- estudar e aplicar métodos de controle e otimização de sistemas não-lineares;
- estudar a metodologia de controle ótimo linear feedback para sistemas não-lineares de tempo contínuo e explorar sua aplicação nos casos de controle contínuo e descontínuo (contínuo por partes);
- estudar e comparar alguns enfoques de sincronização de sistemas caóticos;
- desenvolver e simular um sistema criptográfico baseado em sistemas dinâmicos caóticos de tempo contínuo;

² *Field programmable gate array*.

³ São conhecidos como “jerk” equações e sistemas que tem a forma $\frac{d^3x}{dt^3} = f\left(\frac{d^2x}{dt^2}, \frac{dx}{dt}, x\right)$.

O texto está dividido e organizado em oito capítulos, da seguinte forma: o capítulo 1 é dedicado a definições e apresentação de ferramentas utilizadas no estudo de sistemas dinâmicos caóticos; o capítulo 2 utiliza os conceitos e métodos apresentados no capítulo 1 para estudar detalhadamente os sistemas de Lorenz, Chen e Lü; o capítulo 3 é devotado a definições pertinentes à temática da sincronização e apresentação de métodos de sincronização; o capítulo 4 apresenta a metodologia do controle ótimo linear feedback para sistemas não-lineares e aplica a metodologia para sincronizar os sistemas considerados no capítulo 2; o capítulo 5 estuda aspectos quantitativos da metodologia do controle ótimo linear feedback (custo do controle e tempo gasto na sincronização); o capítulo 6 apresenta simulações numéricas de sincronização de sistemas caóticos via controle linear feedback contínuo por partes; o capítulo 7 utiliza os conceitos trabalhados nos capítulos anteriores e contextualiza a aplicação da sincronização de sistemas caóticos e, finalmente, o capítulo 8 apresenta a aplicação da sincronização de caos à comunicação segura.

1 SISTEMAS DINÂMICOS CONTÍNUOS E CAOS

1.1 Introdução

Um *sistema* pode ser definido como um conjunto de objetos interdependentes agrupados de forma coerente e de forma que exista algum tipo de interação ou relação de causa e efeito entre si. Um sistema é *dinâmico* quando uma ou mais grandezas (que caracterizam seus objetos) variam no tempo [54].

Os *sistemas caóticos* constituem uma classe de sistemas dinâmicos que possui comportamento bastante peculiar, caracterizado pela aparente confusão e desordem. Ledo engano, contudo. Sistemas caóticos, em geral, descrevem trajetórias e fenômenos altamente organizados e complexos.

Este capítulo será dedicado ao estudo de elementos importantes para a compreensão do caos, e tem por objetivo:

- contextualizar o caos historicamente;
- introduzir definições e conceitos fundamentais no estudo de sistemas dinâmicos caóticos;
- caracterizar o caos determinístico;
- apresentar ferramentas utilizadas para o estudo de sistemas caóticos;

1.2 A descoberta do Caos

Apesar de ter sido desenvolvida majoritariamente durante o século XX, a Henri Poincaré, matemático francês do século XIX, pertence o primeiro registro documentado de contato com um sistema de regime caótico. Com o seu famoso “problema dos três corpos”, Poincaré chegou a resultados e a conclusões nunca antes registradas a respeito do comportamento de um sistema dinâmico caótico [8, 29].

O problema dos três corpos foi uma variação do problema da “interação entre dois corpos”, proposto por Isaac Newton. Como as equações de Newton para dois corpos eram passíveis de resolução analítica e de validação experimental, as leis da mecânica clássica pareciam ser o código irrevogável que descrevia de maneira precisa e inequívoca o

comportamento do universo. Assim surgiu o determinismo causal, crença de que, conhecendo-se as leis que regem o universo e o estado do universo em determinado instante, seria possível conhecer o passado ou futuro a qualquer tempo [29].

Pierre Simon Laplace, grande matemático do século XVIII e notório entusiasta do determinismo causal, chegou a afirmar que “*podemos ver o estado presente do universo como o efeito do passado e a causa do futuro*”. Essa afirmação provocou e ainda provoca fervoroso debate filosófico e religioso acerca de temas como a liberdade de escolha e livre-arbítrio, que não podem existir em um mundo regido por causa e efeito [8, 29].

Nesse contexto, o questionamento de Poincaré repercutiu enormemente em sua época, a ponto de um prêmio ser oferecido pela solução do seu problema dos três corpos. Ironicamente, o próprio Poincaré recebeu o prêmio ao provar que o problema não poderia ser resolvido analiticamente. Poincaré surpreendeu-se com órbitas “*tão embaraçadas que eu não posso nem começar a desenhá-las*” [29].

Poincaré também observou que, para condições iniciais minimamente diferentes, as órbitas dos três corpos traçariam caminhos drasticamente diferentes, e então escreveu “*pode acontecer que essas pequenas diferenças na posição inicial conduzam a enormes diferenças no fenômeno final. A previsão se torna impossível*”, sendo essa a primeira frase publicada a respeito da propriedade básica que define um sistema dinâmico caótico: a sensibilidade às condições iniciais [29, 62, 70].

Inquestionavelmente correta, a conclusão de Poincaré inadvertidamente abalou o universo perfeitamente ordenado e determinístico de Newton e Laplace. A ciência da existência de elementos que não se encaixavam no conhecimento filosófico e matemático da época perturbou a comunidade científica, que acreditava ter desvendado o segredo do funcionamento do universo [29].

Já no século XX, em meados de 1963, décadas após o descobrimento de Poincaré, eis que o caos ressurgiu diante dos olhos de Edward Lorenz, meteorologista pesquisador do MIT⁴.

Em uma época em que a meteorologia vivia um momento de descrença, motivada pela produção de resultados “*que variavam de confusos a horríveis*” [29], o surgimento de computadores digitais prometia maior capacidade de cálculo e, como

⁴ Massachusetts Institute of Technology, Cambridge, Massachusetts – EUA.

consequência, a possibilidade de implementação de modelos mais sofisticados para a previsão do tempo. Contudo, essa medida não resolveu o problema e, passada uma década, a meteorologia continuava a obter resultados ruins. Assim, ficou claro que o problema não estava nos modelos matemáticos utilizados.

Através simulações numéricas realizadas com um modelo simples de três equações diferenciais ordinárias, obtidas através da simplificação de um modelo baseado nas equações de Navier-Stokes⁵, Lorenz teve a perspicácia de perceber que estava diante de algo completamente novo, ainda que cada vez mais longe do objetivo original de seu trabalho. Aveso a frustrar-se e abandonar o projeto, Lorenz dedicou-se a entender o que estava acontecendo, e acabou redescobrimo o caos e a sensibilidade às condições iniciais.

Lorenz chamou-a de “*the butterfly effect*”, ou “efeito borboleta”, expressão para a qual Lorenz atribuiu o significado de que uma borboleta, ao bater as asas no Brasil, dispara uma reação em cadeia que pode conduzir a um tornado no Texas algumas semanas mais tarde. Em 1963, em um periódico sobre meteorologia, ele chamou o fenômeno de “*fluxo determinístico não-periódico*”, rebatizado *caos* aproximadamente 13 anos depois pelo físico americano James Yorke.

1.3 Sistemas dinâmicos contínuos, pontos fixos e estabilidade

Os conceitos e definições de sistema contínuo, de estabilidade orbital e estabilidade estrutural são apresentados nesta seção porque constituem fundamentos da teoria do controle e programação dinâmica e essas, por sua vez, constituem parte central deste trabalho. Os conceitos apresentados a seguir são baseados em [1, 10, 11, 18, 23, 26, 54].

Definição 1: *Seja $f(\cdot)$ uma função contínua e diferenciável definida num conjunto compacto⁶ $M \subset \mathbb{R}^m$. Para $x \in M$ a equação $\dot{x} = f(x)$ representa um sistema dinâmico contínuo.*

⁵ Equações que descrevem o movimento de substâncias fluidas tais como líquidos e gases.

⁶ Em um espaço euclidiano, um conjunto é compacto se é fechado e limitado.

Definição 2: Um sistema dinâmico é dito autônomo se as funções que o definem não dependem explicitamente do tempo. Dessa forma, o sistema $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$ é autônomo, enquanto o sistema $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, t)$ é dito não-autônomo.

Pontos Fixos. Os pontos fixos de um sistema dinâmico são os pontos em que a taxa de variação das trajetórias é nulo. Intuitivamente, podemos entendê-los como pontos estacionários, ou seja, pontos das trajetórias onde o movimento cessa.

Definição 3: Num sistema autônomo $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$, os pontos \mathbf{x}^* para os quais $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}^*) = 0$ são chamados de pontos fixos, pontos de equilíbrio, pontos críticos ou pontos estacionários. Se um sistema em equilíbrio sofrer uma pequena perturbação, suas trajetórias podem (a) voltar ao ponto fixo, (b) afastar-se do ponto fixo ou (c) mover-se em uma vizinhança do ponto fixo, porém sem voltar a ele.

Definição 4: Um ponto fixo \mathbf{x}^* de um sistema de tempo contínuo $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$ é um atrator se existe $\delta > 0$ tal que, para uma trajetória $\mathbf{x}(t, \mathbf{x}_0)$ com $\|\mathbf{x}_0 - \mathbf{x}^*\| < \delta$,

$$\lim_{t \rightarrow \infty} \mathbf{x}(t, \mathbf{x}_0) = \mathbf{x}^*.$$

Estabilidade e Estabilidade assintótica. A localização e a estabilidade dos pontos de equilíbrio de um sistema dinâmico autônomo influenciam o retrato de fases do sistema. Assim, para um fluxo $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$, existem pontos de equilíbrio \mathbf{x}^* para os quais $\mathbf{f}(\mathbf{x}^*) = 0$, ou seja, soluções para as quais o sistema pára de se mover no espaço, conhecidas como soluções estacionárias [26, 54]. A estabilidade de um ponto de equilíbrio diz respeito ao comportamento da trajetória que passa próxima a esse ponto.

Seja um sistema de equações diferenciais ordinárias

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}), \quad (1)$$

e seja \mathbf{x}^* um ponto de equilíbrio do sistema (1) tal que

$$\mathbf{f}(\mathbf{x}^*) = 0. \quad (2)$$

Um ponto de equilíbrio é chamado *estável* (segundo Lyapunov) se a resposta do sistema a uma pequena perturbação permanece pequena quando $t \rightarrow \infty$; nesse caso, dizemos que da mesma forma, um ponto de equilíbrio chamado *instável, repulsor, fonte ou "source"* se a perturbação cresce quando $t \rightarrow \infty$.

Definição 5: Um ponto crítico \mathbf{x}^* do sistema (1) é chamado *estável* se, dado qualquer $\varepsilon > 0$, existe $\delta > 0$ tal que toda solução $\mathbf{x} = \boldsymbol{\phi}(t)$ do sistema (1), que em $t = 0$ satisfaz

$$\|\boldsymbol{\phi}(0) - \mathbf{x}^*\| < \delta, \quad (3)$$

existe e satisfaz

$$\|\boldsymbol{\phi}(t) - \mathbf{x}^*\| < \varepsilon, \quad (4)$$

para todo $t \geq 0$.

Um ponto de equilíbrio é chamado *assintoticamente estável, sorvedouro ou "sink"* se a resposta do sistema a uma pequena perturbação aproxima-se de \mathbf{x}^* quando $t \rightarrow \infty$.

Definição 6: Um ponto crítico \mathbf{x}^* é dito *assintoticamente estável* se ele é *estável* e se existe δ_0 , com $0 < \delta_0 < \delta$, tal que se uma solução $\mathbf{x} = \boldsymbol{\phi}(t)$ satisfaz

$$\|\boldsymbol{\phi}(0) - \mathbf{x}^*\| < \delta_0, \quad (5)$$

então

$$\lim_{t \rightarrow \infty} \boldsymbol{\phi}(t) = \mathbf{x}^*. \quad (6)$$

Definição 7: Um ponto crítico \mathbf{x}^* é dito *instável* se ele não é *estável*.

De acordo com [58], sistemas dinâmicos não-lineares podem ser aproximados localmente por um sistema linear, ou seja, podemos linearizar um sistema em torno de seus pontos de equilíbrio e assim investigar sua estabilidade. Na linearização em torno de um ponto fixo \mathbf{x}^* calcula-se a matriz Jacobiana do sistema nesse ponto.

Considere o sistema na forma

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}), \quad (7)$$

onde $f : R^n \rightarrow R^n$ é um campo vetorial não-linear. Se $f(\mathbf{x}^*) = 0$, então \mathbf{x}^* é um ponto fixo do sistema (7). O comportamento da trajetória do sistema perto desse ponto estacionário pode ser determinado pelos autovalores da matriz

$$J_f(\mathbf{x}^*) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \dots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \dots & \frac{\partial f_2}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \dots & \frac{\partial f_n}{\partial x_n} \end{pmatrix} \quad (8)$$

calculada no ponto \mathbf{x}^* . Para que o ponto de equilíbrio seja estável, todos os autovalores devem ter parte real negativa, o que é equivalente a dizer que todas as raízes da equação característica da matriz jacobiana calculada no ponto \mathbf{x}^* devem ter parte real negativa (ver critério de Routh-Hurwitz, no anexo A).

Estabilidade estrutural e Bifurcações. De acordo com [26 , 54], a estabilidade estrutural é fundamentalmente diferente da estabilidade no sentido de Lyapunov no sentido de sua investigação. Enquanto a estabilidade no sentido de Lyapunov é investigada perturbando-se as condições iniciais, a estabilidade estrutural investiga a robustez do retrato de fases sob uma perturbação dos parâmetros de (1). Assim, um sistema é considerado estruturalmente estável se, para qualquer perturbação suficientemente pequena das equações que o definem, o conjunto das órbitas resultantes é topologicamente equivalente⁷ àquele das equações sem a perturbação [26].

Apresentamos a seguir uma definição formal para estabilidade estrutural, baseada em [54].

Definição 8: *Seja o fluxo $\dot{\mathbf{x}} = \mathbf{f}_\mu(\mathbf{x})$, que depende dos parâmetros $\boldsymbol{\mu} = (\mu_1, \mu_2, \dots, \mu_k)$.*

Para um valor fixo dos parâmetros $\boldsymbol{\mu} = \boldsymbol{\mu}_0$, o fluxo $\dot{\mathbf{x}} = \mathbf{f}_{\boldsymbol{\mu}_0}(\mathbf{x})$ é estruturalmente estável se existe $\delta > 0$ tal que $\dot{\mathbf{x}} = \mathbf{f}_\mu(\mathbf{x})$ é topologicamente equivalente a $\dot{\mathbf{x}} = \mathbf{f}_{\boldsymbol{\mu}_0}(\mathbf{x})$, para todos os valores de $\boldsymbol{\mu}$ tais que $\|\boldsymbol{\mu} - \boldsymbol{\mu}_0\| < \delta$.

⁷ Intuitivamente, dois espaços são topologicamente equivalentes se podem ser continuamente deformados, até que um se transforme no outro, sem cortar ou colar.

O comportamento dinâmico de um sistema pode sofrer mudanças significativas ao sofrer perturbações em seus parâmetros, e isso pode ser ilustrado através de um sistema dinâmico linear bidimensional na forma

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mu), \quad (9)$$

onde $\mu \in R$ é um parâmetro de controle, de forma que as soluções do sistema, assim como matrizes jacobianas, autovalores e autovetores também dependem de μ .

Analisando a matriz jacobiana em torno de um ponto fixo, existe a possibilidade de obterem-se autovalores complexos conjugados

$$\lambda_{1,2} = \alpha(\mu) \pm i\beta(\mu). \quad (10)$$

Da teoria da estabilidade de sistemas, concluímos que o foco pode ser estável ou instável, dependendo do sinal de α . Como α é uma função de μ , segue que, variando o valor de μ , podemos passar de um foco estável para um foco instável quando μ atinge um valor crítico μ_c . Nesse momento, diz-se que o sistema sofre uma bifurcação, e μ_c é um ponto de bifurcação.

Quando uma bifurcação ocorre, as órbitas do sistema mudam qualitativamente, ou seja, a topologia do retrato de fases torna-se não-equivalente à original. Nessas condições, pontos estacionários podem perder a estabilidade e novos pontos estacionários podem aparecer [26].

Em outras palavras, chama-se bifurcação à mudança no número de soluções de uma equação diferencial quando um parâmetro é variado [7]. De acordo com [26], a ocorrência de bifurcações é uma característica de sistemas que exibem caos.

Método Direto de Lyapunov. O método direto de Lyapunov, também conhecido como segundo método de Lyapunov, permite investigar a estabilidade de um sistema sem que seja necessário obter sua solução.

As definições e teoremas a seguir são baseados em [10, 11, 26, 54].

Definição 9: Uma função escalar $V(\mathbf{x})$ é chamada definida positiva no conjunto Ω se e somente se $V(\mathbf{0}) = 0$ e $V(\mathbf{x}) > 0$ para $\mathbf{x} \neq \mathbf{0}$ e $\mathbf{x} \in \Omega$.

Definição 10: Uma função escalar $V(\mathbf{x})$ é chamada definida negativa no conjunto Ω se e somente se $-V(\mathbf{x})$ é definida positiva em Ω .

Definição 11: A derivada de V com respeito ao sistema $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$ é o produto escalar

$$\dot{V}(\mathbf{x}) = \text{grad}V(\mathbf{x}) \cdot \mathbf{f}(\mathbf{x}) = \frac{\partial V}{\partial x_1} f_1(\mathbf{x}) + \frac{\partial V}{\partial x_2} f_2(\mathbf{x}) + \dots + \frac{\partial V}{\partial x_n} f_n(\mathbf{x}). \quad (11)$$

Enunciamos a seguir, sem provar, os teoremas formulados por Lyapunov acerca da estabilidade de pontos fixos:

Teorema 1: Suponha que o sistema autônomo $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$ possua um ponto crítico isolado na origem. Se existe uma função escalar definida positiva $V(\mathbf{x})$ tal que $\dot{V}(\mathbf{x}) \leq 0$ (ou seja, não-positiva) em uma região Ω contendo a origem, então a origem é um ponto crítico estável.

Teorema 2: Suponha que o sistema autônomo $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$ possua um ponto crítico isolado na origem. Se existe uma função escalar definida positiva $V(\mathbf{x})$ tal que $\dot{V}(\mathbf{x}) < 0$ em uma região Ω contendo a origem, então a origem é um ponto crítico assintoticamente estável.

Teorema 3: Suponha que o sistema autônomo $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$ possua um ponto crítico isolado na origem. Se existe uma função escalar $V(\mathbf{x})$, $V(\mathbf{0}) = 0$, tal que $\dot{V}(\mathbf{x})$ é definida positiva ou definida negativa em uma região Ω contendo a origem e se existe, em uma vizinhança N da origem, $N \subset \Omega$, pelo menos um ponto \mathbf{a} tal que $V(\mathbf{a})$ possui o mesmo sinal de $\dot{V}(\mathbf{x})$, então a origem é um ponto crítico instável.

1.4 Expoentes característicos de Lyapunov

Os expoentes característicos de Lyapunov determinam a taxa de divergência de trajetórias vizinhas. O número de expoentes de um sistema é igual à dimensão de seu

espaço de fase. Os expoentes são ordenados em ordem decrescente de valor, de forma que para um espaço de fases n -dimensional, temos $\lambda_1, \lambda_2, \dots, \lambda_n$, com $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ [19].

Considere uma hiper-esfera n -dimensional de condições iniciais centrada num ponto $\mathbf{x}(t_0) = \mathbf{x}_0$, de raio inicial $d_i(t_0)$ em cada uma das n dimensões. Com o passar do tempo, a hiper-esfera se deforma, e podemos medir essa deformação em um instante t relacionando o raio no momento t , dado por $d_i(t)$ com o raio inicial $d_i(t_0)$. Assumindo que o raio tenha variado exponencialmente no tempo, temos

$$d_j(t) = d_j(t_0)e^{\lambda_j(t-t_0)}. \quad (12)$$

Que pode ser reescrita como

$$\lambda_j = \frac{\ln[d_j(t)/d_j(t_0)]}{t-t_0}. \quad (13)$$

Os números λ_j são os *expoentes de Lyapunov* [26]. Para um sistema *conservativo*, temos

$$\sum_{j=1}^n \lambda_j = 0 \quad (14)$$

e, por outro lado, para um sistema *dissipativo*

$$\sum_{j=1}^n \lambda_j < 0. \quad (15)$$

Geometricamente, podemos entender os expoentes de Lyapunov como a o comprimento de linhas que separam trajetórias e tem variação $e^{\lambda t}$; como variação de áreas, no caso bidimensional ($e^{(\lambda_1+\lambda_2)t}$), volumes no tridimensional ($e^{(\lambda_1+\lambda_2+\lambda_3)t}$), e etc [19, 26].

A existência de regime caótico é caracterizada pela existência de pelo menos um expoente de Lyapunov positivo. O expoente positivo é que caracteriza dependência sensível às condições iniciais; o expoente ao longo da trajetória é nulo, e o expoente negativo é maior em módulo do que o positivo, para que o sistema seja dissipativo [26].

Os expoentes de Lyapunov também permitem identificar o tipo de atrator encontrado em um sistema. Tomando um sistema tridimensional e considerando os sinais dos expoentes $(\lambda_1, \lambda_2, \lambda_3)$ temos um *ponto fixo* quando $(-, -, -)$, um *ciclo limite* quando $(0, -, -)$, um *toro bidimensional* quando $(0, 0, -)$ e um *atrator estranho* quando $(+, 0, -)$.

1.5 Dissipatividade e o divergente

Seja um volume de condições iniciais V_0 , delimitado em um espaço de fases. Com o objetivo de estudar o que acontece a esse volume na medida em que um sistema desempenha, toma-se uma superfície fechada $S(t)$ de volume $V(t)$ no espaço de fases, de forma que os pontos em S e em seu interior são as condições iniciais das trajetórias. Com a evolução do sistema durante um tempo dt , $S(t)$ evolui para uma nova superfície $S(t+dt)$ e, como consequência, tem-se um novo volume $V(t+dt)$ [54]. A taxa de variação do volume $V(t)$ quando $t \rightarrow \infty$ pode ser medida pelo *divergente* de seu campo vetorial \mathbf{f} .

Teorema 4: *um sistema é conservativo se o divergente do campo vetorial \mathbf{f}*

$$\operatorname{div} \mathbf{f} = \nabla \cdot \mathbf{f} = \frac{\partial f_1}{\partial x_1} + \frac{\partial f_2}{\partial x_2} + \dots + \frac{\partial f_n}{\partial x_n} \quad (16)$$

é nulo, ou seja, $\nabla \cdot \mathbf{f} = 0$. Da mesma forma, se $\nabla \cdot \mathbf{f} < 0$, o sistema é dissipativo, e se $\nabla \cdot \mathbf{f} > 0$, o sistema é expansivo.

Podemos definir sistema conservativo intuitivamente como um sistema cujas trajetórias preservam o volume V_0 com o passar do tempo, de tal modo que o volume ocupado permanece inalterado. Em contrapartida, num sistema dissipativo o volume se contrai, ou seja, em determinado tempo $t > 0$, $V_0 > V_t$.

1.6 Atratores Estranhos

O termo atrator remete à idéia de sistemas dinâmicos dissipativos e intuitivamente podemos definir atrator como um conjunto invariante⁸ para o qual órbitas próximas convergem após um tempo suficientemente longo [26].

Assim como sistemas dissipativos em geral possuem regiões geométricas limitadas do espaço de fases para onde as trajetórias podem convergir, sistemas caóticos

⁸ Uma entidade é considerada invariante a uma transformação se a imagem da transformação da entidade é indistinguível da identidade original.

possuem *atratores estranhos* em seus espaços de fase. Com base em [6, 23], pode-se definir atrator estranho, sistema caótico e dependência sensível de condições iniciais da forma a seguir:

Definição 12: Um atrator é chamado estranho se:

- é limitado;
- qualquer trajetória que inicia no atrator é uma trajetória instável segundo Lyapunov.

As linhas de fluxo de um atrator estranho são sensitivamente dependentes das condições iniciais, ou seja, trajetórias arbitrariamente próximas divergem após um intervalo de tempo suficientemente longo, ficando confinadas em uma região limitada do espaço.

A Figura 1 apresenta o bilhar de Sinai, que constitui-se em um exemplo de sistema caótico com formidáveis propriedades didáticas. Desconsiderando-se o atrito e assumindo todas as colisões dos sistemas como perfeitamente elásticas, é possível observar o desempenho radicalmente diferente dos dois sistemas, apesar de iniciados com condições iniciais levemente diferentes.

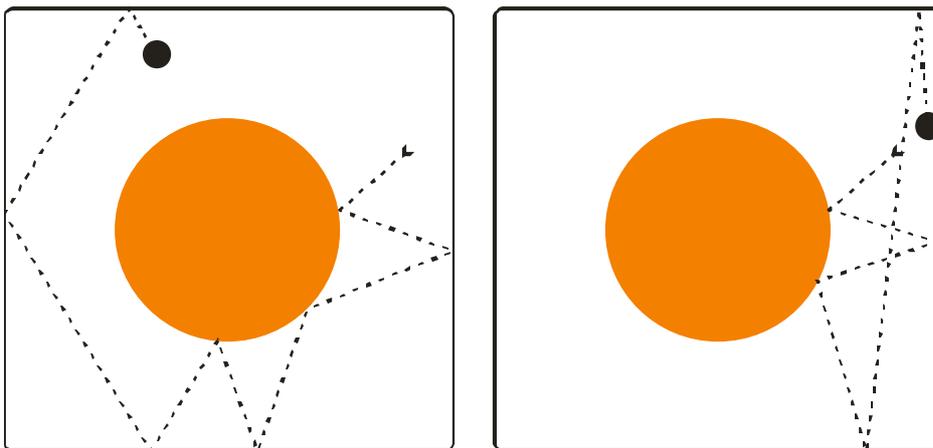


Figura 1 - Bilhar de Sinai com condições iniciais minimamente diferentes

Em um sistema caótico, todos os pontos de equilíbrio são instáveis. Dessa forma, as trajetórias de um sistema caótico tendem para uma região limitada do espaço de

fase, devido à dissipatividade. Por outro lado, as trajetórias não estabilizam-se em um ponto de equilíbrio porque todos os pontos de um sistema caótico são instáveis. Assim, a trajetória permanece confinada em uma região limitada do espaço, o atrator estranho.

1.7 Mapas e Seção de Poincaré

Considere um sistema dinâmico n -dimensional, com soluções periódicas

$$\dot{x} = f(x), \quad (17)$$

onde $f \in R^n$ é um vetor de funções não-lineares. Seja x_0 uma órbita associada a um fluxo φ_t que é solução de (17) e seja $\Omega \subset R^n$ uma hipersuperfície de dimensão $(n-1)$, transversal a esse fluxo. Seja $U \subset \Omega$ o conjunto de pontos onde a órbita intercepta a hipersuperfície Ω . À hipersuperfície Ω dá-se o nome de seção de Poincaré, e o conjunto U é o mapa de Poincaré correspondente.

Conforme [26], um fluxo φ_t de um sistema dinâmico contínuo não-linear pode dar origem a um mapa da forma

$$x_{i+1} = F_\mu(x_i), \quad (18)$$

onde x é um vetor n -dimensional, F é uma função não linear com parâmetro de controle μ e i representa passos temporais fixos e discretos ou passagens sucessivas por uma superfície de seção do fluxo.

De acordo com [7], a seção de Poincaré proporciona uma simplificação do espaço de fases, ao mesmo tempo em que conserva suas propriedades essenciais. O mapa de Poincaré é uma ferramenta muito útil no estudo de órbitas que “rodopiam” próximas a soluções periódicas de sistemas dinâmicos.

1.8 Caracterização do caos determinístico

A sensibilidade às condições iniciais é a característica fundamental de um sistema caótico. Sensibilidade significa que as órbitas de dois sistemas idênticos com condições iniciais x_0 e $x_0 + \varepsilon$, respectivamente, com ε arbitrariamente pequeno, divergirão uma da outra muito rapidamente no espaço de fases [7].

De acordo com [26], algumas características qualitativas do caos determinístico são:

- a imprevisibilidade
- o espectro contínuo de frequências, ou seja, o comportamento aperiódico;
- a invariança da escala, ou seja, estruturas hierárquicas com características de auto-similaridade;
- a estacionaridade, ou seja, a tendência de repetição dos padrões, aperiodicamente.

Um sistema caótico é imprevisível na prática devido à sua dependência sensível das condições iniciais. Essa dependência faz com que as não-linearidades do sistema amplifiquem exponencialmente diferenças arbitrariamente pequenas nas condições iniciais e conduzam a estados completamente distintos após um intervalo suficientemente longo de tempo.

Assim, como é impossível na prática realizar medições com precisão infinita, a incerteza da previsão aumenta até se tornar da ordem da própria amplitude do movimento do sistema. Dessa forma, “*mesmo conhecendo o comportamento do sistema por um tempo arbitrariamente longo, não se pode, ao menos de imediato, prever seu comportamento futuro*” [26].

A seguir, com base em [2, 7, 22, 23, 26, 54], apresentamos as condições para que um sistema dinâmico seja caótico e as condições para que um sistema dinâmico tenha dependência sensível às condições iniciais.

Definição 13: *Um sistema é chamado caótico se possui pelo menos um atrator estranho.*

Definição 14: *Seja $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$ um sistema de tempo contínuo e seja \mathbf{x}_0 um ponto do domínio de $\mathbf{f}(\cdot)$. Se existe $d > 0$ tal que qualquer vizinhança $\{\mathbf{x} : \|\mathbf{x} - \mathbf{x}_0\| < d\}$ de \mathbf{x}_0 contém pelo menos um ponto \mathbf{x}_* tal que $\|\mathbf{f}(\mathbf{x}_0) - \mathbf{f}(\mathbf{x}_*)\| \geq d$ para algum $t_* > 0$, então a órbita $\mathbf{x}(\mathbf{x}_0)$ tem dependência sensível das condições iniciais.*

Definição 15: Uma órbita de um sistema dinâmico de tempo discreto ou de tempo contínuo é dita caótica se ela:

1. possui dependência sensível às condições iniciais;
2. é aperiódica.

Teorema 5: A órbita de um sistema dinâmico discreto ou contínuo tem dependência sensível às condições iniciais se e somente se seu maior expoente de Lyapunov é positivo, ou seja, $\lambda_1 > 0$.

Teorema 6: A órbita de um sistema dinâmico discreto ou contínuo é caótica se, e somente se: (a) seu maior expoente de Lyapunov é positivo; (b) ela é aperiódica.

De acordo com [7, 46], são condições necessárias para a existência de dinâmica caótica em sistemas autônomos de tempo contínuo:

- (a) que o sistema tenha pelo menos três variáveis dinâmicas independentes;
- (b) que as equações do movimento contenham um termo não-linear que acople várias das variáveis.
- (c) que o sistema seja dissipativo;
- (d) que todos os pontos de equilíbrio do sistema sejam instáveis.

De acordo com [54], regime caótico só pode ocorrer em espaços de dimensão $n \geq 3$. Isso ocorre porque o espaço tridimensional é o mínimo suficiente para permitir:

- (a) divergência entre as trajetórias;
- (b) confinamento do movimento em uma região finita do espaço de fases das variáveis dinâmicas;
- (c) unicidade da trajetória.

1.9 Considerações finais

O método direto de Lyapunov, apresentado na seção 1.3, é imprescindível no estudo de sistemas não-lineares porque permite concluir a respeito da estabilidade ou

instabilidade do sistema sem que seja necessário obter sua solução. Além disso, a teoria da estabilidade de Lyapunov é um dos pilares da Teoria do controle em que se baseia o controle ótimo linear feedback, que será apresentado no capítulo 4.

Por sua vez, os expoentes de Lyapunov e o mapa de Poincaré fornecem resultados conclusivos a respeito da existência de regime caótico, ao mesmo tempo em que são métodos cuja utilização é direta⁹ e cuja teoria subjacente pode ser abordada intuitivamente de maneira relativamente descomplicada. Por esse motivo, esses métodos foram escolhidos para o estudo dos sistemas de Lorenz, Chen e Lü, apresentado no capítulo 2.

As definições e teoremas apresentados neste capítulo objetivaram proporcionar entendimento e clareza dos conceitos pertinentes ao caos, de forma que estejam presentes todas as vezes em que forem revisitados ao longo do texto.

⁹ No sentido *straightforward*.

2 ESTUDO DOS MODELOS MATEMÁTICOS

2.1 Introdução

O presente capítulo utiliza ferramentas e conceitos apresentados e discutidos no capítulo anterior para estudar três sistemas caóticos: os sistemas de Lorenz, Chen e Lü, que são casos especiais de um sistema mais geral, chamado *Generalized Lorenz-Like System* [46, 48, 49, 73], ou sistema de Lorenz generalizado. Em adição, o capítulo apresenta também o sistema caótico unificado que unifica os três sistemas através da inclusão de um parâmetro α , de forma que para $\alpha = 0$ obtem-se o sistema de Lorenz, para $\alpha = 0,8$ e $\alpha = 1$, o sistema de Lü e o sistema de Chen, respectivamente.

Os principais objetivos do capítulo são:

- determinar as condições de dissipatividade e existência do atrator;
- determinar as condições de existência e de estabilidade dos pontos fixos;
- investigar a existência de caos nos sistemas através do mapa de Poincaré e expoentes de Lyapunov;
- confirmar a existência de regime caótico no sistema caótico unificado para todo o intervalo $\alpha \in [0,1]$.

De acordo com [46], para que um sistema seja caótico, é necessário que ele seja dissipativo e que todos os seus pontos de equilíbrio sejam instáveis. Dessa forma, a determinação das condições de estabilidade dos pontos fixos dos sistemas tem o intuito de obter as condições de instabilidade dos pontos fixos, tendo em vista cumprir a condição necessária para o caos.

2.2 Sistema de Lorenz

De acordo com [19], o sistema de Lorenz é um modelo para a descrição do movimento do fluxo de um fluido turbulento em uma *célula de Rayleigh-Bénard*

*idealizada*¹⁰. Assim, considerando a situação ideal, complicadas equações diferenciais parciais que descrevem a dinâmica do fluido e temperatura são simplificadas e se tornam um sistema de três equações diferenciais ordinárias, representado pelas equações

$$\begin{aligned}\dot{x}_1 &= \sigma(x_2 - x_1) \\ \dot{x}_2 &= rx_1 - x_2 - x_1x_3 \\ \dot{x}_3 &= x_1x_2 - bx_3\end{aligned}\tag{19}$$

onde $(x_1, x_2, x_3) \in \mathbb{R}^3$ são funções cujos significados físicos são: $x_1(t)$ é proporcional à intensidade da convecção, $x_2(t)$ é proporcional à diferença de temperatura entre as correntes de fluido ascendente e descendente; e $x_3(t)$ é proporcional à distorção do perfil de temperatura vertical, relativamente a um perfil linear, e $(\sigma, r, b) \in \mathbb{R}^3$ são parâmetros, onde $\sigma, b, r > 0$. Originalmente, $(\sigma, r, b) = (10, 28, 8/3)$.

O parâmetro σ depende das propriedades do fluido (tipicamente 0,7 para um gás ideal, de 1 a 4 para água e de 10 a 1000 para óleos); o parâmetro b depende do comprimento de onda horizontal ou diâmetro de rolamento na célula; o parâmetro r representa a diferença de temperatura entre as paredes fria e quente da célula [19].

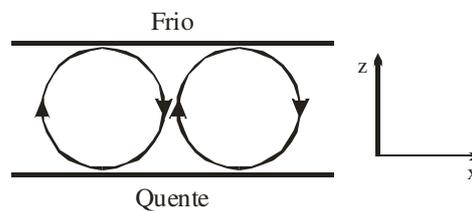


Figura 2 - Esquema da célula de Rayleigh-Bénard

Ainda de acordo com [19], as equações do sistema de Lorenz apresentam algumas características importantes:

- são autônomas, ou seja, t não aparece explicitamente nas equações;
- envolvem somente derivadas de primeira ordem;
- possuem duas não-linearidades;
- são dissipativas;
- as soluções são limitadas.

¹⁰ Na célula idealizada, é considerado que a célula estende-se indefinidamente para frente e para trás, para a direita e para a esquerda, sendo aquecida embaixo e resfriada em cima.

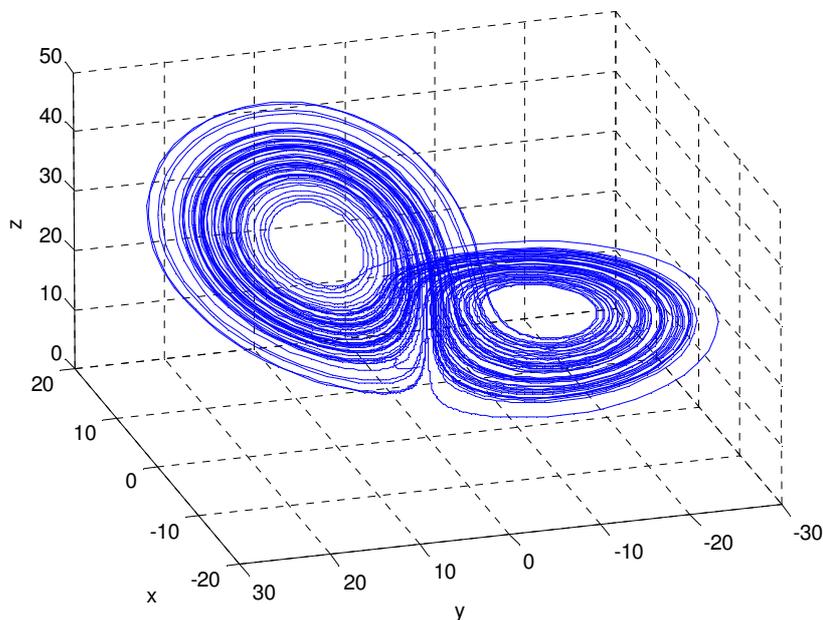


Figura 3 - Atrator de Lorenz

Dissipatividade e existência do atrator. Um atrator estranho somente surge em sistemas dissipativos, e nesse sentido investigamos a dissipatividade do sistema de Lorenz. Aplicando a equação (16) ao sistema (19), obtêm-se:

$$\nabla V = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} = -(\sigma + b + 1)$$

Como $\nabla V = -(\sigma + b + 1) < 0$, então o sistema de Lorenz é dissipativo.

O elemento de volume V_0 é contraído em um elemento de volume $V_0 e^{-(\sigma+b+1)t}$, e isso significa que quando $t \rightarrow \infty$, o volume que contém a trajetória do sistema é reduzido a zero. Assim, todas as órbitas do sistema estão confinadas num subconjunto de volume zero, e esse movimento assintótico se estabelece em um atrator.

Pontos fixos e estabilidade. Tomando-se (19), fazendo $\dot{x}_1 = \dot{x}_2 = \dot{x}_3 = 0$ e resolvendo o sistema resultante, obtemos os pontos fixos P_1 , P_2 e P_3 . Para $0 < r \leq 1$ existe um único ponto fixo P_1 ; para $r > 1$ surgem outros dois pontos fixos, P_2 e P_3 .

$$\begin{aligned}
P_1 &= (x_1^*, x_2^*, x_3^*) = (0, 0, 0), \\
P_2 &= (x_1^*, x_2^*, x_3^*) = (\sqrt{b(r-1)}, \sqrt{b(r-1)}, r-1) e \\
P_3 &= (x_1^*, x_2^*, x_3^*) = (-\sqrt{b(r-1)}, -\sqrt{b(r-1)}, r-1).
\end{aligned} \tag{20}$$

Calculando a matriz Jacobiana J para cada ponto de equilíbrio, obtemos

$$\begin{aligned}
J_{P_1} &= \begin{pmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{pmatrix}, \\
J_{P_2} &= \begin{pmatrix} -\sigma & \sigma & 0 \\ 1 & -1 & -\sqrt{b(r-1)} \\ \sqrt{b(r-1)} & \sqrt{b(r-1)} & -b \end{pmatrix}, \\
J_{P_3} &= \begin{pmatrix} -\sigma & \sigma & 0 \\ 1 & -1 & \sqrt{b(r-1)} \\ -\sqrt{b(r-1)} & -\sqrt{b(r-1)} & -b \end{pmatrix}.
\end{aligned}$$

A seguir, investigamos o valor dos parâmetros para os quais os pontos fixos são estáveis, isto é, para os quais a parte real dos autovalores das matrizes jacobianas J é negativa.

Calculando o determinante da matriz jacobiana para o ponto de equilíbrio P_1 ,

$$|J_{P_1}| = \begin{vmatrix} -\sigma - \lambda & \sigma & 0 \\ r & -1 - \lambda & 0 \\ 0 & 0 & -b - \lambda \end{vmatrix} = 0,$$

obtemos a equação característica

$$f_{P_1}(\lambda) = -(\sigma + \lambda)(1 - \lambda)(b + \lambda) + \sigma r(b + \lambda) = 0.$$

Como fica claro que $\lambda = -b$ é um autovalor, a equação se reduz a:

$$\begin{aligned}
f_{P_1}(\lambda) &= -(\sigma + \lambda)(1 + \lambda) + \sigma r = 0 \\
&= \lambda^2 + (\sigma + 1)\lambda + \sigma(r - 1) = 0.
\end{aligned}$$

Aplicando-se o critério de Routh-Hurwitz¹¹, obtemos que se a condição

$$r < 1 \tag{21}$$

¹¹ Ver detalhes do critério de Routh-Hurwitz no anexo A [66].

é satisfeita, então $\lambda_1 < 0$, $\lambda_2 < 0$, $\lambda_3 < 0$, e a origem é um ponto de equilíbrio estável. Considerando o significado físico das equações de Lorenz, é possível afirmar que para $r < 1$ não há convecção.

Calculando o determinante da matriz jacobiana para o ponto P_2

$$|J_{P_2}| = \begin{vmatrix} -\sigma - \lambda & \sigma & 0 \\ 1 & -1 - \lambda & -\sqrt{b(r-1)} \\ \sqrt{b(r-1)} & \sqrt{b(r-1)} & -b - \lambda \end{vmatrix} = 0,$$

obtemos a equação característica

$$\begin{aligned} f_{P_2}(\lambda) &= -(\sigma + \lambda)(1 + \lambda)(b + \lambda) - \sigma b(r - 1) + \sigma(b + \lambda) - b(\sigma + \lambda)(r - 1) = 0 \\ &= -\lambda^3 - (\sigma + b + 1)\lambda^2 - (b(\sigma + r))\lambda - 2\sigma b(r - 1) = 0. \end{aligned}$$

Aplicando o critério de Routh-Hurwitz, obtemos que se as condições

$$-(\sigma + b + 1) < 0 \text{ (dissipatividade)}, \quad (22)$$

$$r > 1 \text{ (existência de } P_2 \text{ e } P_3) \text{ e} \quad (23)$$

$$r - 1 < \frac{(\sigma + r)(\sigma + b + 1)}{2\sigma} \quad (24)$$

são satisfeitas, então P_2 é um ponto de equilíbrio estável.

Considerando que o sistema (19) é invariante sob a transformação $(x, y, z) \rightarrow (-x, -y, z)$, é possível concluir que se a condição (24) é satisfeita, então o ponto de equilíbrio P_3 também é estável.

De acordo com [46] para que o sistema (19) tenha comportamento caótico, é necessário que:

- o sistema (19) seja dissipativo, ou seja, $\nabla V = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} < 0$;
- o sistema (19) tenha três pontos de equilíbrio instáveis.

Considerando as conclusões a respeito de dissipatividade e estabilidade do sistema, podemos concluir que, para que o sistema (19) seja caótico, é necessário que as condições $-(\sigma + b + 1) < 0$ (dissipatividade), $r > 1$ (instabilidade do ponto fixo trivial e existência dos pontos fixos não-triviais) e $r - 1 > \frac{(\sigma + r)(\sigma + b + 1)}{2\sigma}$ (instabilidade dos pontos fixos não-triviais) sejam satisfeitas.

Expoentes de Lyapunov. A Figura 4 apresenta o gráfico dos expoentes de Lyapunov do sistema (19) para os parâmetros originais. O valor e o sinal dos expoentes permitem concluir que o sistema é dissipativo e, como consequência, que suas trajetórias ficam confinadas em um atrator estranho.

A Figura 5, e a Figura 6 mostram os valores dos expoentes de Lyapunov em função do parâmetro r . É possível observar o momento em que um dos expoentes se torna positivo, o que significa nesse contexto o surgimento do caos.

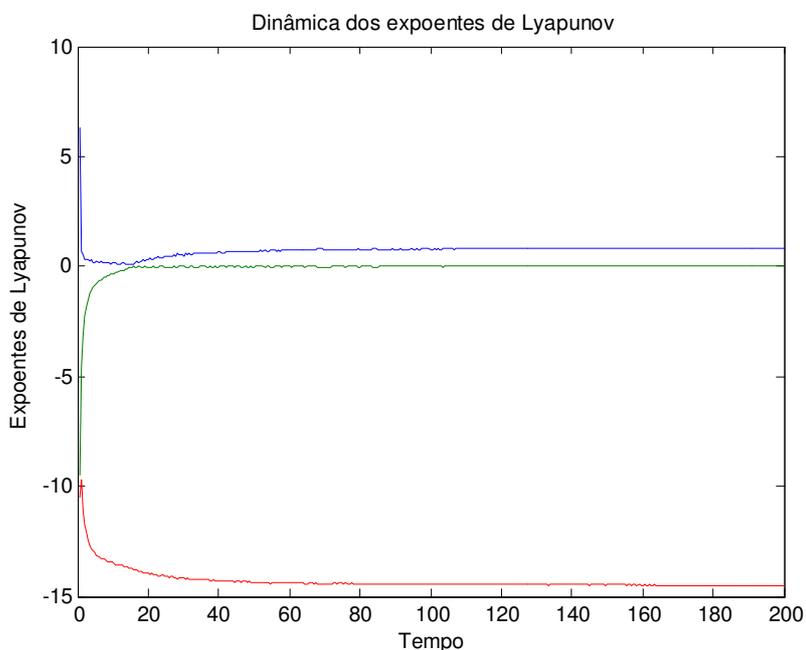


Figura 4 - Expoentes de Lyapunov do sistema de Lorenz

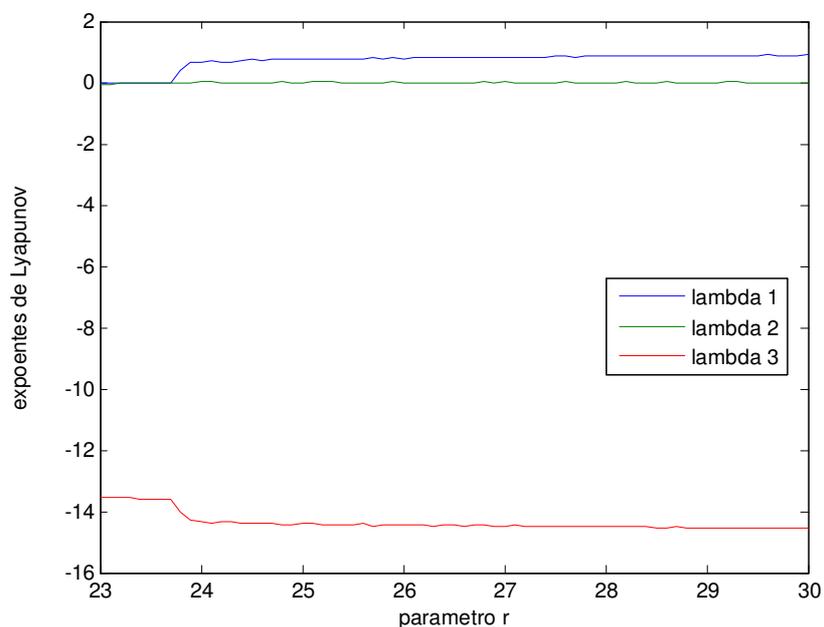


Figura 5 - Dinâmica dos expoentes de Lyapunov – Sistema de Lorenz

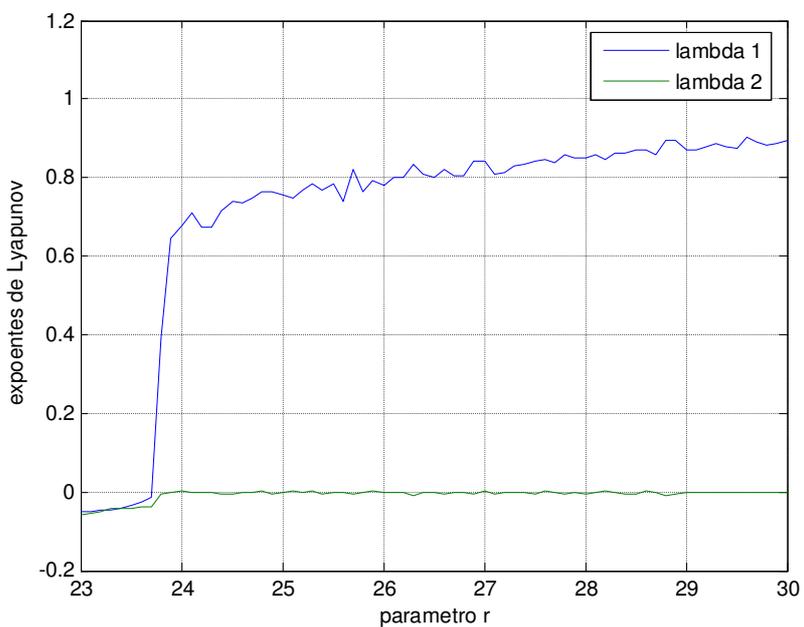


Figura 6 - Dinâmica dos expoentes de Lyapunov (zoom em λ_1 e λ_2) – Sistema de Lorenz

Seção de Poincaré. A seção de Poincaré do sistema de Lorenz é apresentada abaixo. Os pontos em preto apresentam a interseção do atrator com o plano $x_1 = 0$.

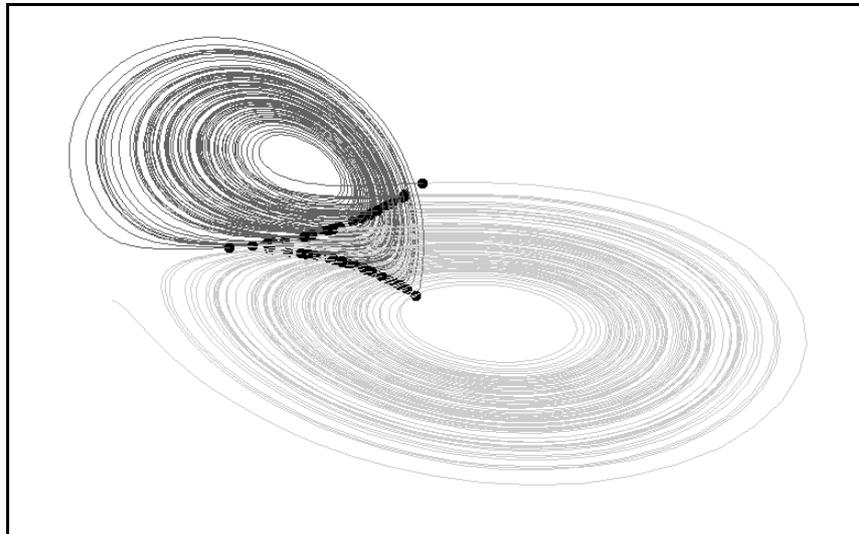


Figura 7 - Seção de Poincaré do sistema de Lorenz

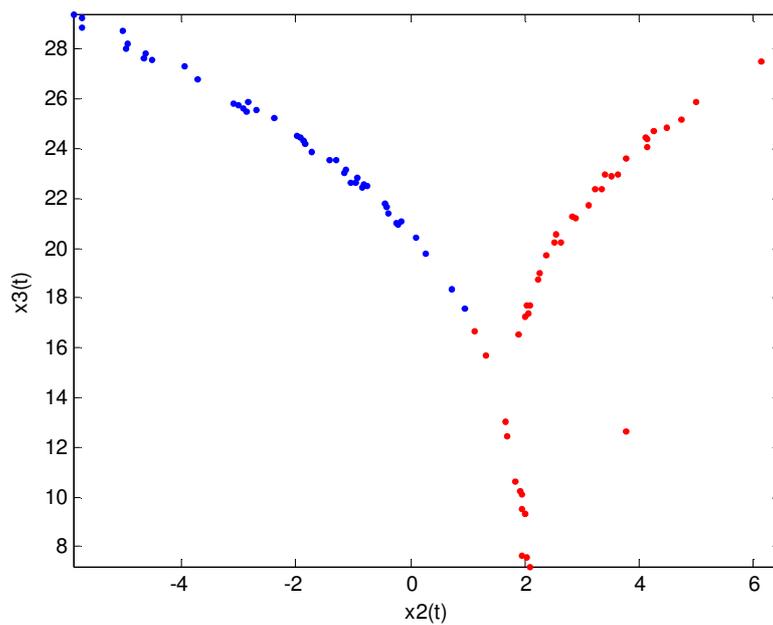


Figura 8 - Mapa de Poincaré do sistema de Lorenz, $x_1=1$

2.3 Sistema de Chen

Descoberto em 1999, o sistema de Chen é um dual do sistema de Lorenz no sentido de que, considerando a matriz $A_{3 \times 3}$ dos termos lineares, o sistema de Lorenz

satisfaz a condição $a_{12}a_{21} > 0$, enquanto o sistema de Chen satisfaz $a_{12}a_{21} < 0$ ¹². O sistema de Chen é dado pelas equações

$$\begin{aligned}\dot{x}_1 &= a(x_2 - x_1) \\ \dot{x}_2 &= (c - a)x_1 + cx_2 - x_1x_3 \\ \dot{x}_3 &= x_1x_2 - bx_3.\end{aligned}\tag{25}$$

Onde $(x_1, x_2, x_3) \in \mathbb{R}^3$ são funções que definem o espaço de fases e $(a, b, c) \in \mathbb{R}^3 / a, b, c \geq 0$ são parâmetros, cujos valores originais são $(35, 3, 28)$. Cabe ressaltar que o sistema de Chen e o valor de seus parâmetros não possuem significado físico.

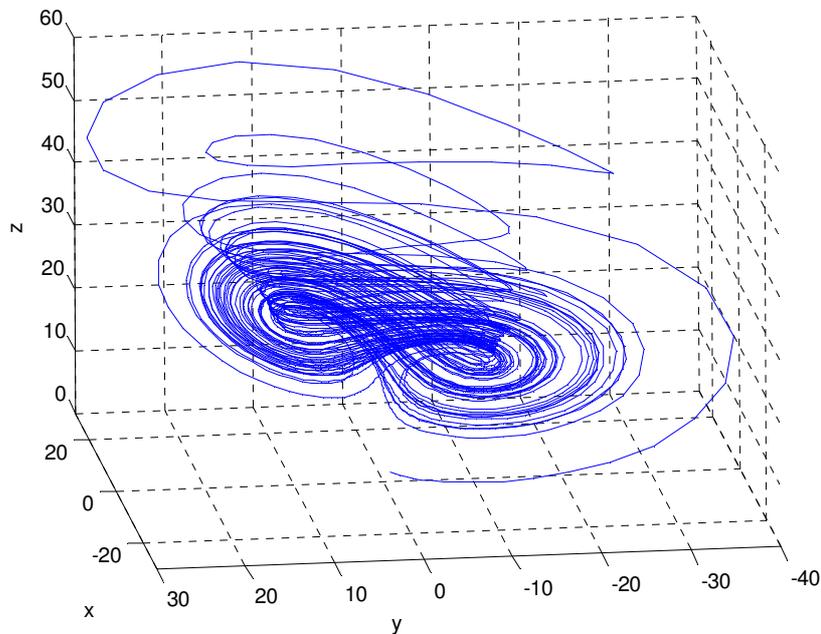


Figura 9 - Atrator de Chen

Dissipatividade e Existência do atrator. Investigamos a seguir a dissipatividade do sistema de Chen. Aplicando a equação (16) ao sistema de Chen, obtemos

$$\nabla V = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} = -a + c - b = -(a + b - c).$$

Pode-se concluir que, para $a + b > c$, o sistema de Chen é dissipativo.

¹² Para maiores detalhes, ver Vanecek & Celikovsky, 1996.

Satisfeita essa condição, o elemento de volume V_0 é contraído em um elemento de volume $V_0 e^{-(a+b-c)t}$, e isso significa que quando $t \rightarrow \infty$, o volume que contem a trajetória do sistema é reduzido a zero. Assim, todas as órbitas do sistema estão confinadas num subconjunto de volume zero, e esse movimento assintótico se estabelece em um atrator.

Pontos fixos e estabilidade. Tomando (25), fazendo $\dot{x}_1 = \dot{x}_2 = \dot{x}_3 = 0$ e resolvendo o sistema resultante, obtemos os pontos fixos P_1 , P_2 e P_3 . Para $2c \leq a$, existe um único ponto fixo P_1 . Para $2c > a$ surgem os pontos fixos P_2 e P_3 .

$$\begin{aligned} P_1 &= (x_1^*, x_2^*, x_3^*) = (0, 0, 0), \\ P_2(x_1^*, x_2^*, x_3^*) &= (\sqrt{b(2c-a)}, \sqrt{b(2c-a)}, 2c-a) e \\ P_3(x_1^*, x_2^*, x_3^*) &= (-\sqrt{b(2c-a)}, -\sqrt{b(2c-a)}, 2c-a). \end{aligned} \quad (26)$$

Calculando a matriz Jacobiana J para cada ponto de equilíbrio, obtemos

$$\begin{aligned} J_{P_1} &= \begin{pmatrix} -a & a & 0 \\ c-a & c & 0 \\ 0 & 0 & -b \end{pmatrix}, \\ J_{P_2} &= \begin{pmatrix} -a & a & 0 \\ -c & c & -\sqrt{b(2c-a)} \\ \sqrt{b(2c-a)} & \sqrt{b(2c-a)} & -b \end{pmatrix}, \\ J_{P_3} &= \begin{pmatrix} -a & a & 0 \\ -c & c & \sqrt{b(2c-a)} \\ -\sqrt{b(2c-a)} & -\sqrt{b(2c-a)} & -b \end{pmatrix}. \end{aligned}$$

A seguir, investigamos o valor dos parâmetros para os quais os pontos fixos são estáveis, isto é, para os quais a parte real dos autovalores das matrizes jacobianas J é negativa.

Calculando o determinante da matriz jacobiana para o ponto de equilíbrio P_1

$$|J_{P_1}| = \begin{vmatrix} -a-\lambda & a & 0 \\ c-a & c-\lambda & 0 \\ 0 & 0 & -b-\lambda \end{vmatrix} = 0.$$

Obtemos a equação característica

$$f_{P_1}(\lambda) = (a + \lambda)(c - \lambda)(b + \lambda) + (b + \lambda)(c - a)a = 0.$$

Como fica claro que $\lambda = -b$ é um autovalor, a equação se reduz a:

$$\begin{aligned} f_{P_1}(\lambda) &= (a + \lambda)(c - \lambda) + (c - a)a = 0 \\ &= -\lambda^2 + (c - a)\lambda + 2ac - a^2 = 0. \end{aligned}$$

Aplicando-se o critério de Routh-Hurwitz, obtemos que se as condições

$$c < a, \quad (27)$$

$$2c < a \quad (28)$$

são satisfeitas, então $\lambda_1 < 0$, $\lambda_2 < 0$, $\lambda_3 < 0$, e a origem é um ponto de equilíbrio estável.

Considerando que $a, b, c > 0$, podemos manter somente a condição mais restritiva. Então, se a condição (28) é satisfeita, P_1 é o único ponto fixo do sistema (25).

Calculando o determinante da matriz jacobiana para o ponto fixo P_2

$$|J_{P_2}| = \begin{vmatrix} -a - \lambda & a & 0 \\ -c & c - \lambda & -\sqrt{b(2c - a)} \\ \sqrt{b(2c - a)} & \sqrt{b(2c - a)} & -b - \lambda \end{vmatrix} = 0,$$

obtemos a equação característica

$$\begin{aligned} f_{P_2}(\lambda) &= (a + \lambda)(c - \lambda)(b + \lambda) - ab(2c - a) - ac(b + \lambda) - (a + \lambda)(2c - a)b = 0 \\ &= -\lambda^3 + (-a - b + c)\lambda^2 + (-bc)\lambda - 4abc + 2a^2b = 0. \end{aligned}$$

Aplicando o critério de Routh-Hurwitz e considerando que o sistema (25) é invariante sob a transformação $(x, y, z) \rightarrow (-x, -y, z)$, é possível concluir que se as condições

$$a + b > c \quad (\text{dissipatividade}), \quad (29)$$

$$2c > a \quad (\text{existência de } P_2 \text{ e } P_3) \text{ e} \quad (30)$$

$$\frac{4ac - 2a^2}{a + b - c} < c \quad (31)$$

são satisfeitas, então P_2 e P_3 são pontos de equilíbrio estáveis.

De acordo com [46], para que o sistema (25) tenha comportamento caótico, é necessário que:

- o sistema (25) seja dissipativo, ou seja, $\nabla V = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} < 0$;
- o sistema (25) tenha três pontos de equilíbrio instáveis.

Considerando as conclusões a respeito de dissipatividade e estabilidade do sistema, podemos concluir que, para que o sistema (25) seja caótico, é necessário que as condições $a+b > c$ (*dissipatividade*), $2c > a$ (*instabilidade do ponto fixo P_1 e existência dos pontos fixos P_2 e P_3*) e $\frac{4ac - 2a^2}{a+b-c} > c$ (*instabilidade dos pontos fixos não-triviais*) sejam satisfeitas.

Expoentes de Lyapunov. A Figura 10 apresenta o gráfico dos expoentes de Lyapunov do sistema (25) para os parâmetros originais. O valor e o sinal dos expoentes permitem concluir que o sistema é dissipativo e que as trajetórias ficam confinadas em um atrator estranho.

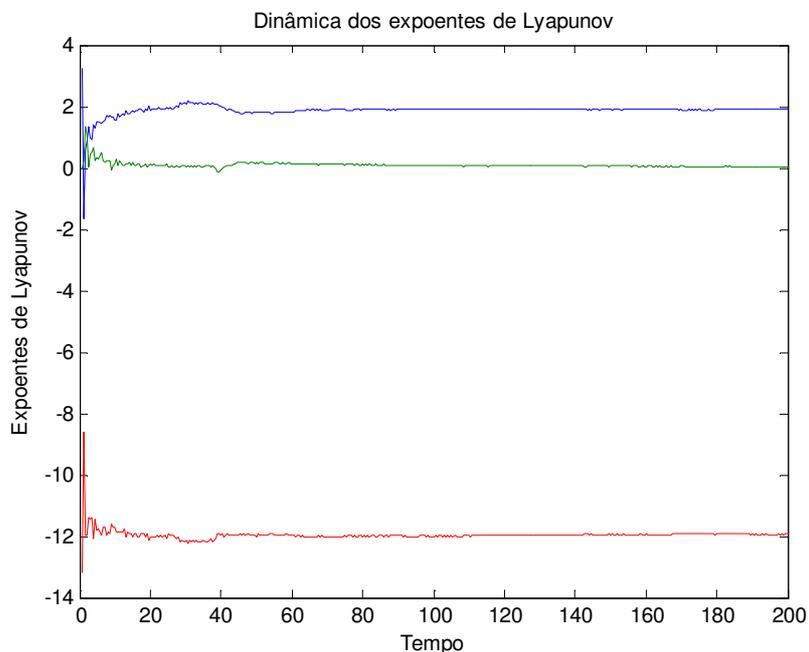


Figura 10 - Expoentes de Lyapunov para o sistema de Chen

A Figura 11 e a Figura 12 apresentam a dinâmica dos expoentes de Lyapunov do sistema de Chen em função do parâmetro c . É possível observar o surgimento do regime caótico quando o maior expoente assume valores maiores que zero.

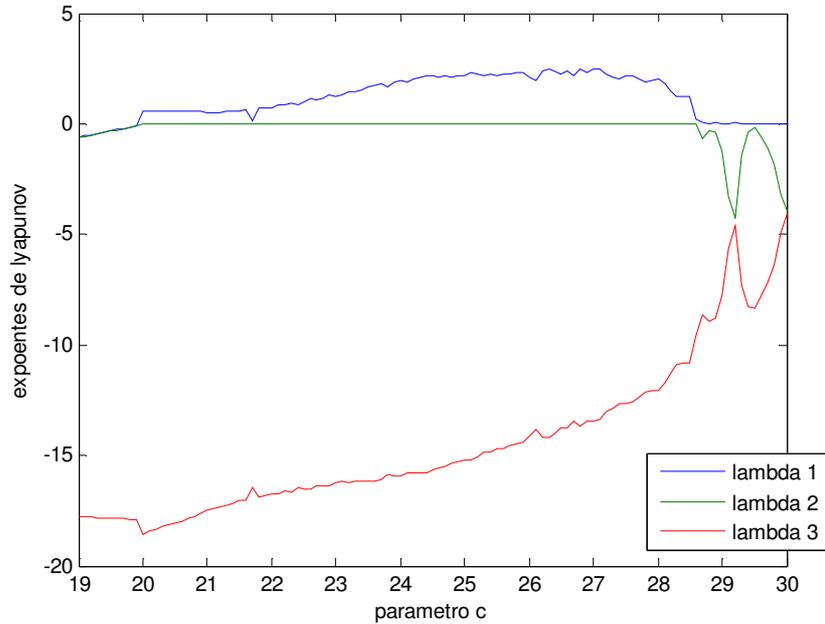


Figura 11 - Dinâmica dos expoentes de Lyapunov

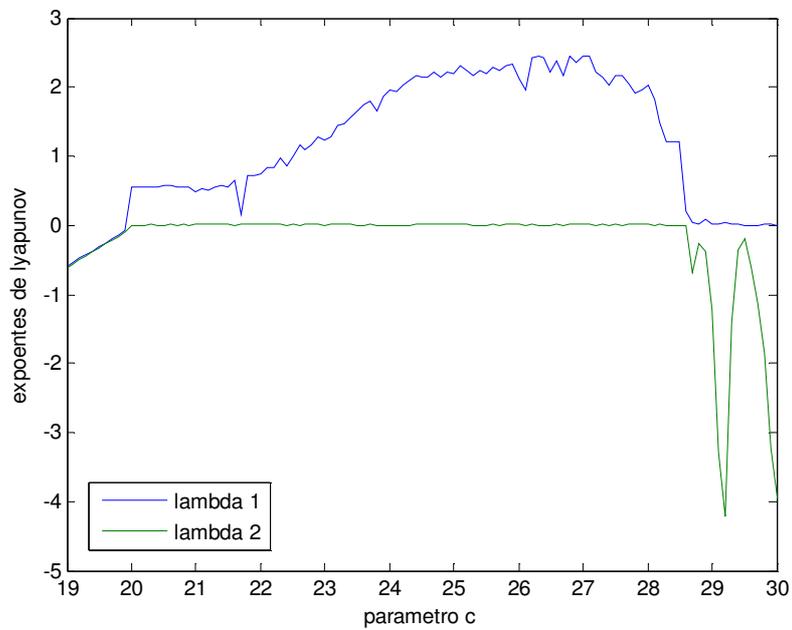


Figura 12 - Dinâmica dos expoentes de Lyapunov (zoom em λ_1 e λ_2)

Seção de Poincaré. A seção de Poincaré do sistema de Chen é apresentada abaixo. Os pontos em preto apresentam a interseção do atrator com o plano $x_1 = 0$.

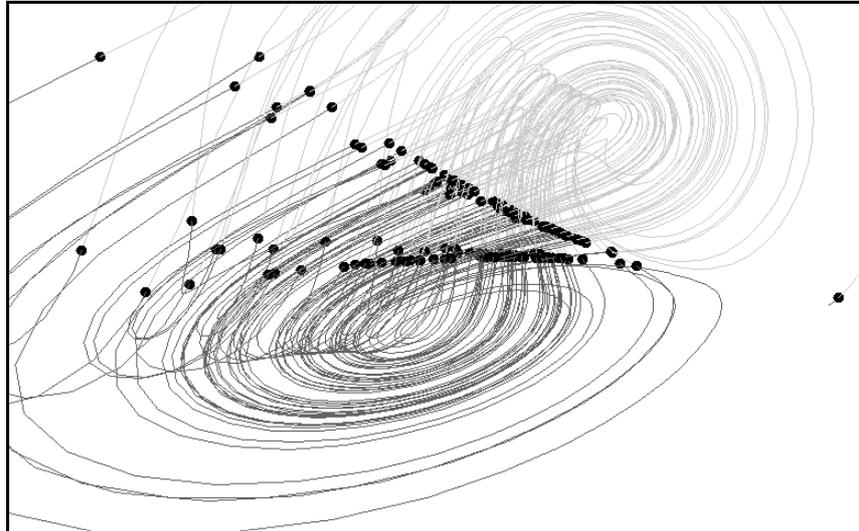


Figura 13 - Seção de Poincaré do sistema de Chen

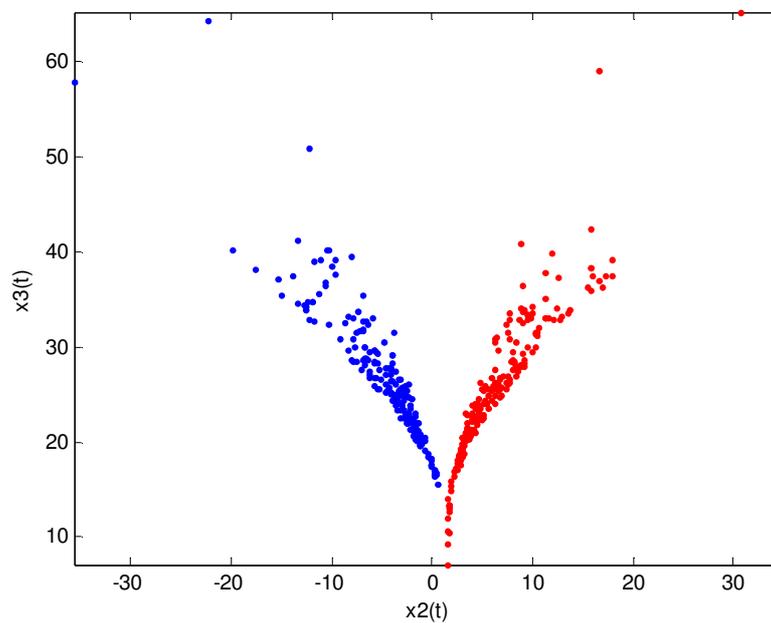


Figura 14 - Mapa de Poincaré do sistema de Chen, $x_1=1$

2.4 Sistema de Lü

O sistema de Lü é um sistema semelhante aos sistemas de Lorenz e Chen, porém seu atrator é topologicamente não-equivalente àqueles. Considerando a matriz $A_{3 \times 3}$

dos termos lineares, o sistema de Lorenz satisfaz à condição $a_{12}a_{21} > 0$, o sistema de Chen satisfaz $a_{12}a_{21} < 0$, e o sistema de Lü satisfaz $a_{12}a_{21} = 0$. O sistema de Lü é dado pelas equações

$$\begin{aligned}\dot{x}_1 &= a(x_2 - x_1) \\ \dot{x}_2 &= cx_2 - x_1x_3, \\ \dot{x}_3 &= x_1x_2 - bx_3\end{aligned}\tag{32}$$

onde $(x_1, x_2, x_3) \in \mathbb{R}^3$ são funções que definem o espaço de fases e $(a, b, c) \in \mathbb{R}^3 / a, b, c > 0$ são parâmetros, cujos valores originais são $(36, 3, 20)$ e não possuem significado físico.

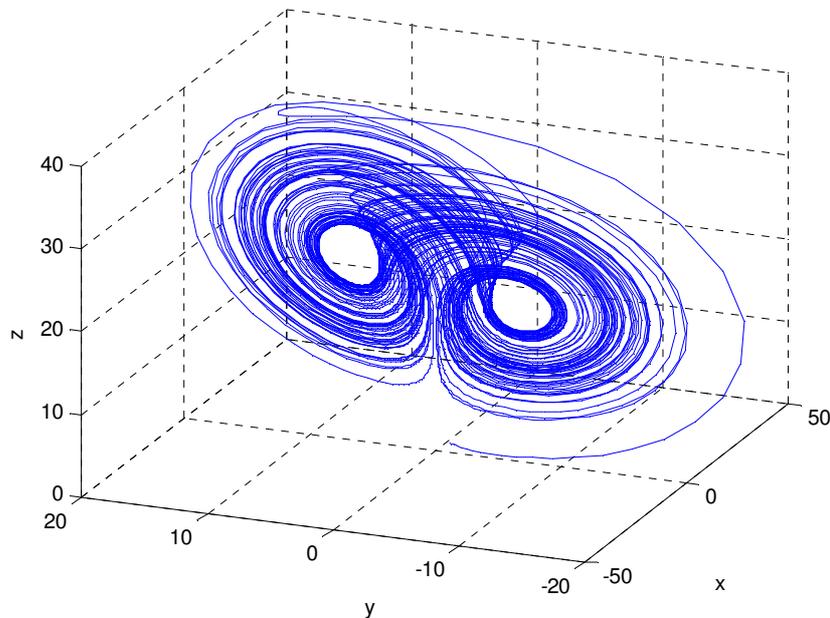


Figura 15 - Atrator de Lü

Dissipatividade e Existência do atrator. Investigamos a seguir a dissipatividade do sistema de Lü. Aplicando a equação (16) ao sistema (32), obtemos

$$\nabla V = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} = -a + c - b = -(a + b) + c$$

Para $a + b > c$, o sistema de Lü é dissipativo.

Satisfeita essa condição, o elemento de volume V_0 é contraído em um elemento de volume $V_0 e^{-(a+b-c)t}$, e isso significa que quando $t \rightarrow \infty$, o volume que contem a trajetória do sistema é reduzido a zero. Assim, todas as órbitas do sistema estão confinadas num subconjunto de volume zero, e esse movimento assintótico se estabelece em um atrator.

Pontos fixos e estabilidade. Tomando-se (32), fazendo $\dot{x}_1 = \dot{x}_2 = \dot{x}_3 = 0$ e resolvendo o sistema resultante, obtemos os pontos fixos P_1 , P_2 e P_3 .

$$\begin{aligned} P_1 &= (x_1^*, x_2^*, x_3^*) = (0, 0, 0), \\ P_2 &(x_1^*, x_2^*, x_3^*) = (\sqrt{bc}, \sqrt{bc}, c) \text{ e} \\ P_3 &(x_1^*, x_2^*, x_3^*) = (-\sqrt{bc}, -\sqrt{bc}, c). \end{aligned} \quad (33)$$

Calculando a matriz Jacobiana J para cada ponto de equilíbrio, obtemos

$$\begin{aligned} J_{P_1} &= \begin{pmatrix} -a & a & 0 \\ 0 & c & 0 \\ 0 & 0 & -b \end{pmatrix}, \\ J_{P_2} &= \begin{pmatrix} -a & a & 0 \\ -c & c & -\sqrt{bc} \\ \sqrt{bc} & \sqrt{bc} & -b \end{pmatrix}, \\ J_{P_3} &= \begin{pmatrix} -a & a & 0 \\ -c & c & \sqrt{bc} \\ -\sqrt{bc} & -\sqrt{bc} & -b \end{pmatrix}. \end{aligned}$$

A seguir, investigamos o valor dos parâmetros para os quais os pontos fixos são estáveis, isto é, para os quais a parte real dos autovalores das matrizes jacobianas J é negativa.

Calculando o determinante para o ponto de equilíbrio P_1

$$f_{P_1}(\lambda) = \begin{vmatrix} -a-\lambda & a & 0 \\ 0 & c-\lambda & 0 \\ 0 & 0 & -b-\lambda \end{vmatrix} = 0,$$

obtemos a equação característica

$$f_{P_1}(\lambda) = (a + \lambda)(c - \lambda)(b + \lambda) = 0.$$

Fica claro que $\lambda_1 = -a$, $\lambda_2 = c$, $\lambda_3 = -b$ são autovalores. Se

$$\begin{aligned} a &> 0, \\ b &> 0 \quad e \\ c &< 0, \end{aligned} \tag{34}$$

então $\lambda_1 < 0$, $\lambda_2 < 0$, $\lambda_3 < 0$, e a origem é um ponto de equilíbrio estável. Se as condições (34) são satisfeitas, então P_1 é o único ponto de equilíbrio do sistema (32).

Calculando o determinante para o ponto fixo P_2

$$f_{P_2}(\lambda) = \begin{vmatrix} -a - \lambda & a & 0 \\ -c & c - \lambda & -\sqrt{bc} \\ \sqrt{bc} & \sqrt{bc} & -b - \lambda \end{vmatrix} = 0,$$

obtemos a equação característica

$$\begin{aligned} f_{P_2}(\lambda) &= (-a - \lambda)(c - \lambda)(-b - \lambda) - abc + ac(-b - \lambda) + bc(-a - \lambda) = 0 \\ &= -\lambda^3 + (-a - b + c)\lambda^2 + (-ab)\lambda - 2abc = 0. \end{aligned}$$

Aplicando o critério de Routh-Hurwitz, obtemos que se as condições

$$a + b > c \quad (\text{dissipatividade}) \tag{35}$$

$$abc > 0 \tag{36}$$

$$\frac{2c}{a + b - c} < 1 \tag{37}$$

são satisfeitas, então P_2 é um ponto de equilíbrio estável.

Considerando que o sistema (25) é invariante sob a transformação $(x, y, z) \rightarrow (-x, -y, z)$, é possível concluir que se as condições (35), (36) e (37) são satisfeitas, então o ponto de equilíbrio P_3 também é estável.

De acordo com [46], para que o sistema (32) tenha comportamento caótico, é necessário que:

- o sistema (32) seja dissipativo, ou seja, $\nabla V = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} < 0$;
- o sistema (32) tenha três pontos de equilíbrio instáveis.

Considerando as conclusões a respeito de dissipatividade e estabilidade do sistema, podemos concluir que, para que o sistema (32) seja caótico, é necessário que as condições $a+b > c$ (*dissipatividade*), $abc > 0$ (*instabilidade do ponto fixo trivial*) e $\frac{2c}{a+b-c} > 1$ (*instabilidade dos pontos fixos não-triviais*) sejam satisfeitas.

Expoentes de Lyapunov. A Figura 16 apresenta o gráfico dos expoentes de Lyapunov do sistema (32) para os parâmetros originais. O valor e o sinal dos expoentes permitem concluir que o sistema é dissipativo e que as trajetórias ficam confinadas em um atrator estranho.

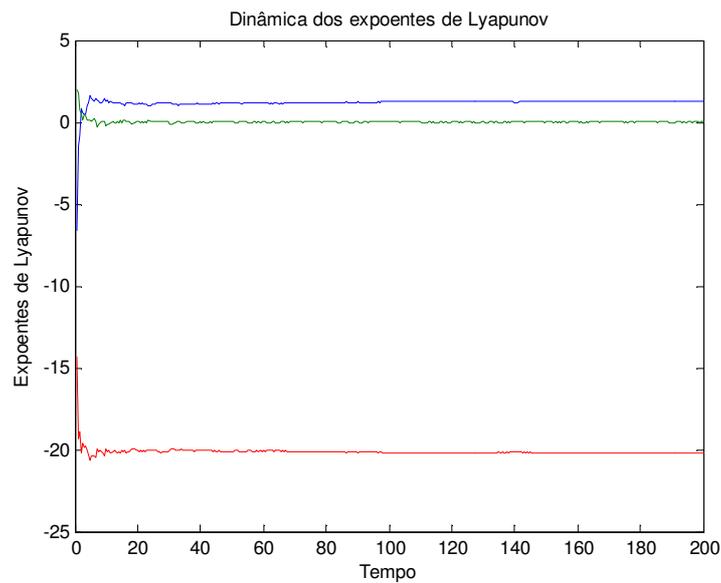


Figura 16 - Expoentes de Lyapunov do sistema de Lü

A Figura 17 e a Figura 18 apresentam a dinâmica dos expoentes de Lyapunov do sistema de Lü em função do parâmetro a . Pode-se observar que o sistema é dissipativo para todo o intervalo $25 \leq a \leq 48$, e caótico para parte dele.

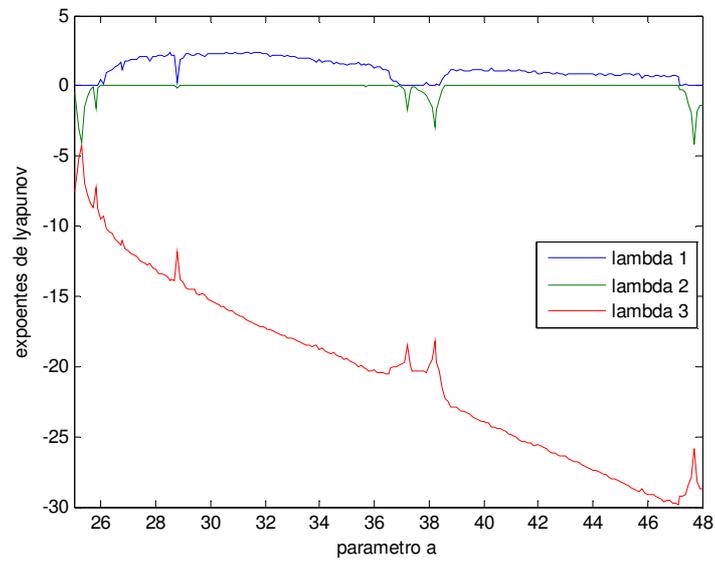


Figura 17 - Dinâmica dos expoentes de Lyapunov

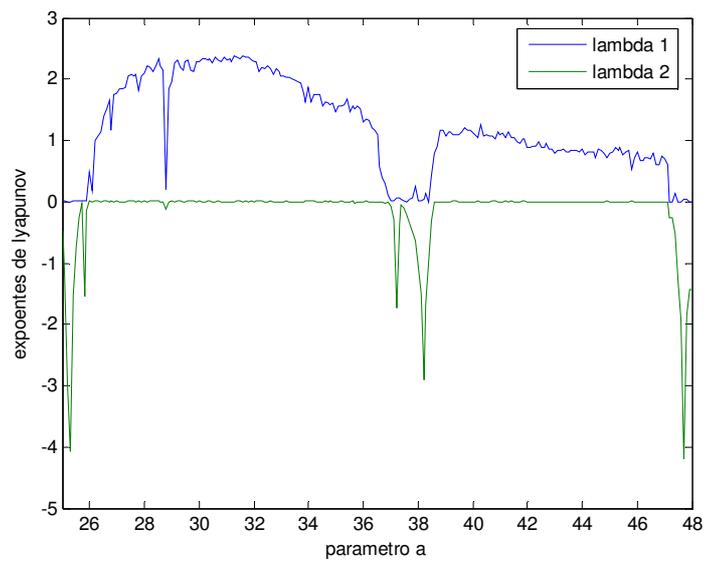


Figura 18 - Dinâmica dos expoentes de Lyapunov (zoom em λ_1 e λ_2)

Seção de Poincaré. A seção de Poincaré do sistema de Lü é apresentada abaixo. Os pontos em preto apresentam a interseção do atrator com o plano $x_1 = 0$.

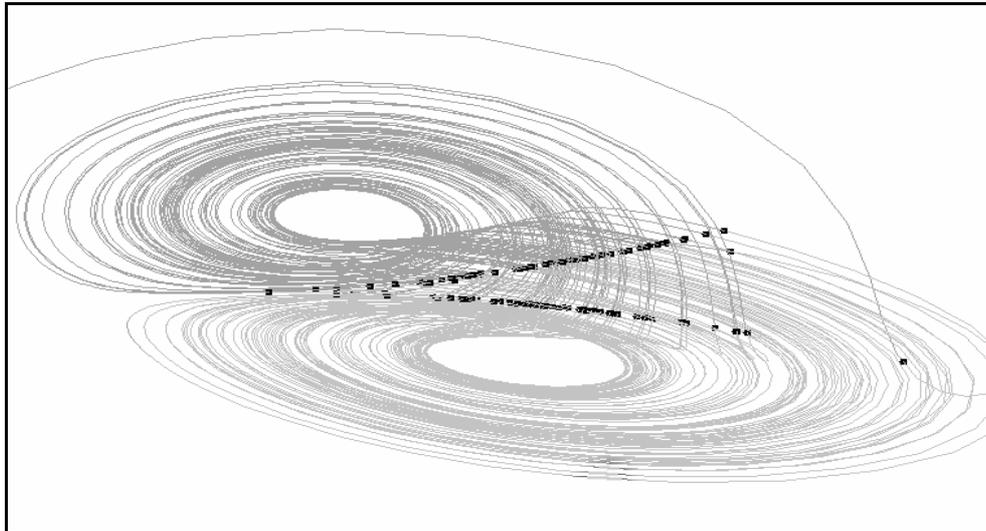


Figura 19 - Seção de Poincaré do sistema de Lü

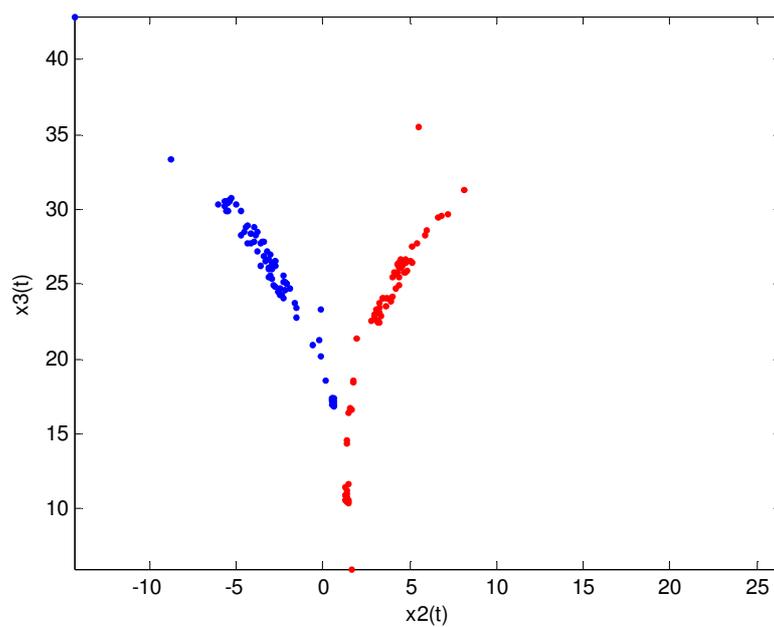


Figura 20 - Mapa de Poincaré do sistema de Lü, $x_1=1$

2.5 Sistema caótico unificado

Lü et al. [50] propuseram um sistema caótico que unifica os sistemas de Lorenz, de Lü e de Chen através da inclusão de um parâmetro $0 \leq \alpha \leq 1$. Para $0 \leq \alpha < 0,8$, o sistema caótico unificado é topologicamente equivalente ao sistema de Lorenz; para

$0,8 < \alpha \leq 1$, é topologicamente equivalente ao sistema de Chen; e para $\alpha = 0,8$ surge um terceiro atrator topologicamente não-equivalente aos outros dois, chamado atrator de Lü. Para todos os valores $0 \leq \alpha \leq 1$ o sistema apresenta comportamento caótico. As equações do sistema caótico unificado são apresentadas abaixo

$$\begin{aligned}\dot{x}_1 &= (25\alpha + 10)(x_2 - x_1) \\ \dot{x}_2 &= (28 - 35\alpha)x_1 - x_1x_3 + (29\alpha - 1)x_2 \\ \dot{x}_3 &= x_1x_2 - \left(\frac{\alpha + 8}{3}\right)x_3\end{aligned}\quad (38)$$

A Figura 21, a Figura 22 e a Figura 23 apresentam os atratores obtidos para simulações do sistema caótico unificado para $\alpha = 0$ (atrator de Lorenz), para $\alpha = 0,8$ (atrator de Lü) e para $\alpha = 1$ (atrator de Chen).

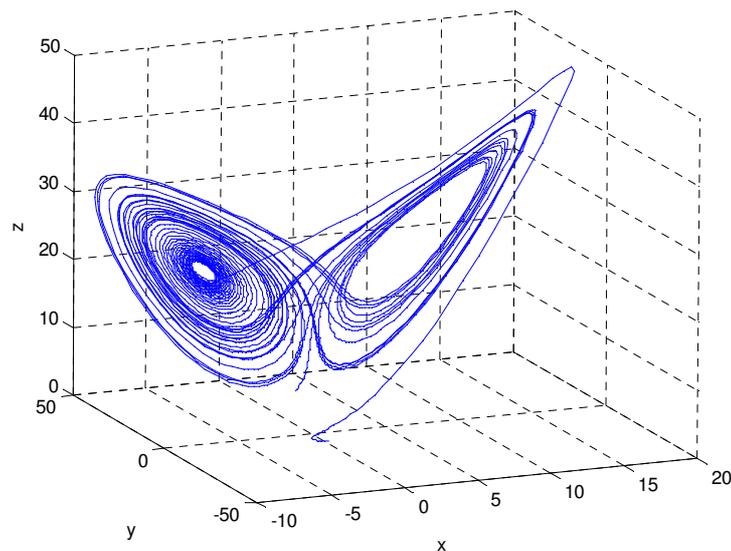


Figura 21 - Atrator de Lorenz, $\alpha=0$

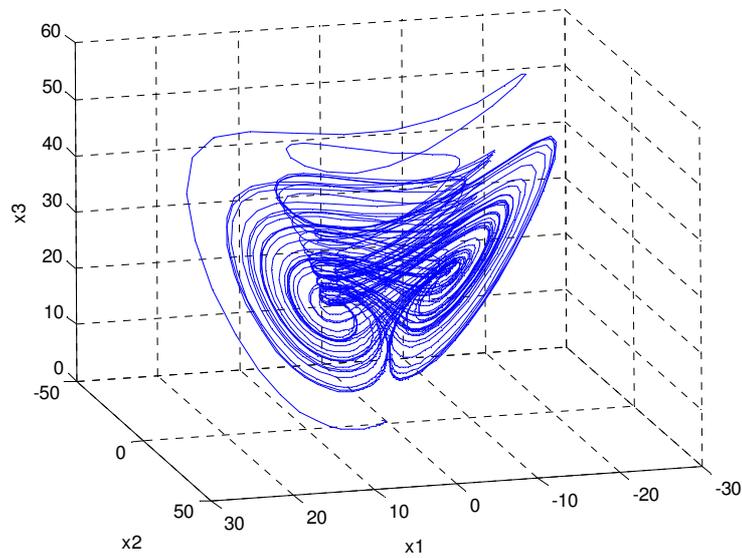


Figura 22 – Atrator de Lü, $\alpha=0,8$

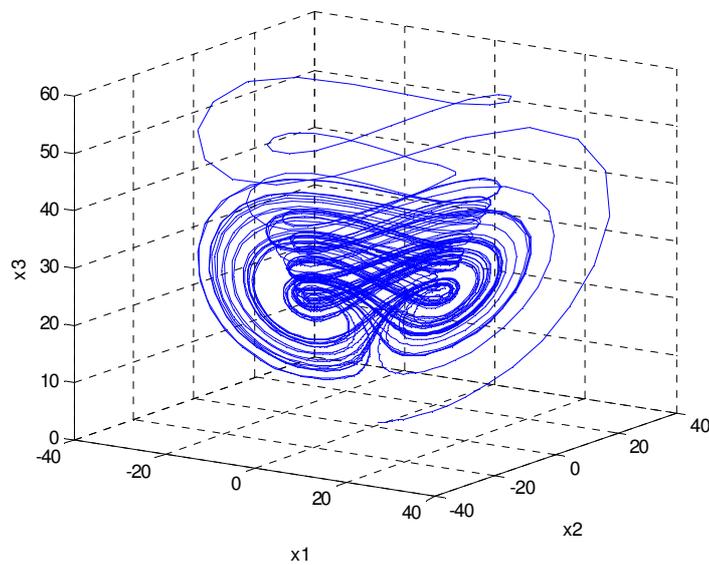


Figura 23 - Atrator de Chen, $\alpha=1$

Expoentes de Lyapunov. A Figura 24 mostra a dinâmica dos expoentes de Lyapunov do sistema caótico unificado para o intervalo $0 \leq \alpha \leq 1$. O sistema unificado é dissipativo e caótico para todo o intervalo considerado.

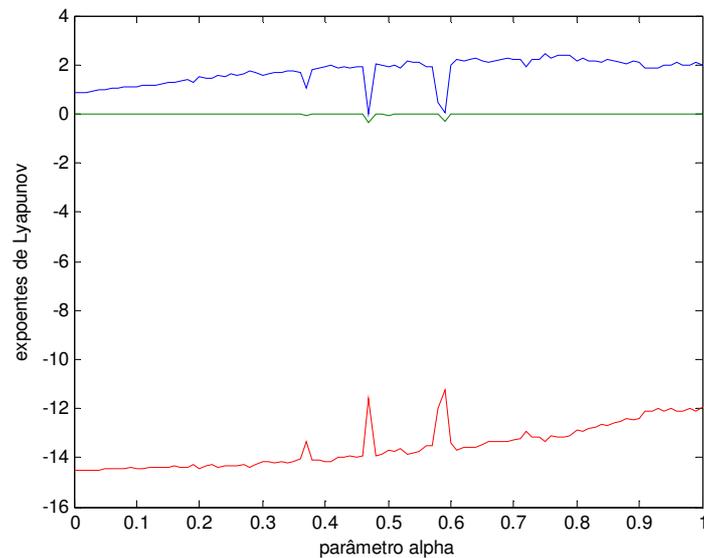


Figura 24 - Expoentes de Lyapunov - sistema caótico unificado

2.6 Considerações finais

A partir da aplicação do divergente e do critério de Routh-Hurwitz, foram obtidas as condições que garantem a dissipatividade dos sistemas e a instabilidade de seus pontos de equilíbrio. Sistemas dissipativos com pontos de equilíbrio instáveis fornecem condições para que as trajetórias se estabeleçam em um atrator sem se estabilizarem em um ponto fixo. Como já foi mencionado anteriormente, tais condições são necessárias para o surgimento do regime caótico [46].

Através da aplicação das ferramentas apresentadas no primeiro capítulo foi possível investigar analítica e numericamente cada um dos sistemas. A partir dos resultados obtidos com o cálculo dos expoentes de Lyapunov, foi possível verificar a existência de caos para uma ampla faixa de parâmetros dos sistemas. No caso do sistema caótico unificado, foi possível comprovar que o regime caótico persiste para todo o intervalo $\alpha \in [0,1]$, sendo este o resultado mais relevante do presente capítulo.

Em [50], Lü et al. enunciam esse mesmo resultado, sem contudo mencionar de que forma fora obtido. Como o sistema caótico unificado será explorado na aplicação proposta no capítulo final deste trabalho, a investigação teve por objetivo repetir de forma independente os resultados publicados em [50] como forma de ratificá-los.

3 SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS

3.1 Introdução

Sincronizar significa tornar sincrônico; combinar movimentos para que se dêem ao mesmo tempo; tornar solidários e simultâneos os movimentos de dois ou mais aparelhos.

É possível estender essa idéia a sistemas caóticos. Dois osciladores caóticos independentes sujeitos a excitações distintas produzirão movimentos não-relacionados com o passar do tempo. Estabelecendo-se um acoplamento entre esses osciladores, de forma que eles se tornem “dependentes” um do outro, existe a possibilidade de que esses osciladores apresentem movimentos *síncronos* com o passar do tempo. Isso significa que eles produzirão movimentos relacionados, e a esse fenômeno dá-se o nome de sincronização. Em se tratando de osciladores caóticos, temos a sincronização de caos ou, conforme o título deste capítulo, *sincronização de sistemas caóticos* [40, 41, 42, 43, 55, 56].

Existem diferentes tipos de sincronização, entre elas a sincronização idêntica (*identical synchronization*), a sincronização generalizada (*generalized synchronization*), a sincronização em fase (*phase synchronization*) e a sincronização com atraso (*lag synchronization*). Dentre estas, abordaremos somente a sincronização idêntica, que ocorre quando dois sistemas acoplados cujas variáveis de estado são $\mathbf{x}, \mathbf{y} \in R^n$ têm condições iniciais $\mathbf{x}(0) = \mathbf{x}_0$ e $\mathbf{y}(0) = \mathbf{y}_0$ e $\|\mathbf{y} - \mathbf{x}\| \rightarrow 0$ na medida em que $t \rightarrow \infty$.

O presente capítulo tem por objetivo:

- introduzir o conceito de sincronização intuitivamente e, em seguida matematicamente;
- introduzir exemplos do fenômeno da sincronização na natureza;
- estudar a sincronização a partir do ponto de vista de alguns enfoques comumente encontrados na literatura.

3.2 Sincronização na natureza

De acordo com [71], são poucas as situações em que se tem um entendimento claro de como a ordem surge espontaneamente, e isso inclui a ordem verificada quando, por exemplo, a água é submetida a temperaturas abaixo do ponto de congelamento e trilhões de moléculas se tornam uma estrutura rígida e simétrica espontaneamente. A baixa temperatura faz com que um fluido com comportamento extremamente complexo se torne uma estrutura ordenada *espacialmente*.

Da mesma forma, existem fenômenos ordenados *temporalmente*, e eles são conhecidos como *sincronização*. A sincronização ocorre em variados tipos de sistemas, vivos ou não, e consiste na simpatia entre dois ou mais osciladores com condições iniciais arbitrariamente diferentes e que passam a comportar-se em “unísono”, ou seja, como se fossem um único grande oscilador. Portanto, podemos definir sincronização intuitivamente como a correlação *temporal* de dinâmicas de sistemas distintos e acoplados [12].

Fenômenos temporalmente ordenados possuem elementos que tornam sua explicação problemática: é preciso medir e comparar as propriedades dos sistemas, verificar a concordância das propriedades no tempo, de que forma os osciladores estão acoplados, ou seja, qual é o estímulo que permite aos osciladores atingirem a sincronização e de que forma isso ocorre [71].

Na natureza, a sincronização de osciladores se apresenta de diversas e fascinantes formas: congregações de milhares de vaga-lumes piscando individual e desordenadamente passam a piscar em unísono, após certo tempo, como se fossem um único e grande vaga-lume; o trabalho ordenado e rítmico das células cardíacas conhecidas como células marca-passo, responsáveis pelo sinal elétrico que rege as pulsações do coração; a sincronização de ciclos menstruais de mulheres sujeitas à convivência prolongada; e a sincronização de relógios de pêndulo suspensos em uma moldura comum e, no mundo microscópico, trilhões de elétrons que marcham ordenadamente por um supercondutor¹³.

Osciladores acoplados e com movimentos inicialmente desorganizados podem sincronizar em duplas, em trios e assim por diante, até que todos os osciladores estejam

¹³ Materiais que conduzem correntes sem resistência nem perdas, quando submetidos a baixíssimas temperaturas, devido às suas características intrínsecas.

sincronizados. Isso ocorre na medida em que cada oscilador sofre a influência dos demais e adianta ou atrasa seu ritmo para adequar-se aos outros sem que exista um líder. De acordo com [71], a inexistência de um líder é uma configuração mais robusta que surge quando, por exemplo, a tarefa de controlar os ritmos cardíacos é confiada a várias células ao invés de somente uma, sujeita à morte e a mau funcionamento.

3.3 Sincronização de caos

Por muito tempo acreditou-se que caos e sincronização fossem fenômenos antagônicos e mutuamente excludentes, devido às características peculiares observadas em um oscilador caótico (sensibilidade às condições iniciais), em contraste à sutileza e organização de osciladores sincronizados.

Com as publicações de Pecora e Carroll [60] e Grebogi, Ott e Yorke [32], a possibilidade de controle e sincronização de osciladores caóticos foi conhecida e a sincronização de caos teve sua conotação, a princípio controversa, alterada. Desde então ela tornou-se objeto de intenso estudo no meio científico.

Assim como a sincronização de osciladores pode ocorrer de forma espontânea, ela pode também ser induzida ou forçada, através de metodologias de controle. Assim, dois ou mais osciladores podem ser levados artificialmente a sincronizarem suas trajetórias. Tal medida justifica-se em aplicações práticas, onde é necessário que a sincronização ocorra e que ela ocorra rapidamente.

Independentemente dos diferentes enfoques com que a sincronização é abordada e ilustrada neste trabalho, utilizaremos a seguinte definição matemática para sincronização de caos:

Definição 16: *Dados dois sistemas dinâmicos caóticos com condições iniciais $\mathbf{x}(0) = \mathbf{x}_0$ e*

$\mathbf{y}(0) = \mathbf{y}_0$ cujas trajetórias são descritas pelas equações diferenciais ordinárias

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) \quad e \quad (39)$$

$$\dot{\mathbf{y}} = \mathbf{f}(\mathbf{y}), \quad (40)$$

onde $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ e $f : \mathbb{R}_n \rightarrow \mathbb{R}_n$ é um campo vetorial não linear, dizemos que os sistemas (39) e (40) estão sincronizados se $\|\mathbf{e}(t)\| = \|\mathbf{y}(t) - \mathbf{x}(t)\| \rightarrow 0$ quando $t \rightarrow \infty$.

3.4 Alguns enfoques da sincronização de caos

O problema da sincronização de sistemas caóticos pode ser abordado a partir de diferentes enfoques. As principais diferenças encontradas entre os enfoques dizem respeito ao tempo necessário para sincronização, à estabilidade do método, ao grau de generalidade com que o problema da sincronização pode ser resolvido e à facilidade de implementação do método.

Um método de sincronização de caos é chamado globalmente estável se conduz as trajetórias dos sistemas à sincronização, independentemente das condições iniciais do sistema escravo. Nesse caso, mesmo que as condições iniciais dos sistemas não façam parte da mesma *bacia de atração*¹⁴, os sistemas se tornarão síncronos.

Se o método de sincronização de caos é composto por um algoritmo que pode ser aplicado a uma grande quantidade de osciladores caóticos diferentes, diz-se que o método possui alto grau de generalidade. Essa característica é importante porque, em geral, significa que novos problemas podem ser resolvidos seguindo-se etapas bem definidas utilizadas em problemas anteriores.

A facilidade de implementação diz respeito à simplicidade com que o problema da sincronização, concebido e resolvido matematicamente, pode ser inserido no contexto prático de uma maneira descomplicada e direta.

Nesta seção, exploramos alguns enfoques frequentemente encontrados na literatura: o *acoplamento*, o *projeto de um sistema observador*, o *controle mestre-escravo*, o *controle não-linear* e o *controle ativo*. Para cada um dos quatro primeiros enfoques, formulamos o problema e apresentamos um exemplo de sincronização do sistema de Lorenz. No quinto e último, apresentamos a sincronização dos sistemas de Chen e Lorenz, conforme metodologia proposta em [30].

¹⁴ Região do espaço de fases que contém um atrator para o qual as órbitas convergem.

As simulações numéricas utilizam o método de Runge-Kutta de 4ª ordem, com

$$\text{passo de integração } h = 10^{-2} \text{ e condições iniciais } \mathbf{x}(0) = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \text{ e } \mathbf{y}(0) = \begin{pmatrix} -2 \\ 1 \\ 3 \end{pmatrix}.$$

Acoplamento ([27, 45]). A sincronização de sistemas caóticos acoplados é baseada na introdução de uma das variáveis de estado do sistema mestre no sistema escravo, que a utiliza como valor de entrada. O acoplamento é a forma como a sincronização geralmente ocorre na natureza, e está ligada à influência que um ou mais sistemas sofrem de sistemas semelhantes. Tal metodologia de sincronização é mostrada a seguir.

Sejam os sistemas mestre (41) e escravo (42)

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}), \quad (41)$$

$$\dot{\mathbf{y}} = \mathbf{f}(\mathbf{y}, x_k) \quad (42)$$

e seja o sistema em desvios

$$\dot{\mathbf{e}} = \dot{\mathbf{y}} - \dot{\mathbf{x}} \quad (43)$$

onde $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ e $k \in \mathbb{N} / k = [1, n]$. Diz-se que os sistemas (41) e (42) estão acoplados pela variável x_k .

A sincronização por acoplamento depende fundamentalmente da forma como os sistemas estão acoplados. Para que a sincronização ocorra, a variável utilizada no acoplamento deve entrar no sistema escravo de forma que o sistema em desvios (43) seja assintoticamente estável segundo Lyapunov. Um exemplo é apresentado a seguir para ilustrar a idéia.

Seja o sistema mestre

$$\begin{aligned} \dot{x}_1 &= -\sigma(x_1 - x_2) \\ \dot{x}_2 &= rx_1 - x_2 - x_1x_3, \\ \dot{x}_3 &= x_1x_2 - bx_3 \end{aligned} \quad (44)$$

e seja o sistema escravo

$$\begin{aligned} \dot{y}_1 &= -\sigma(y_1 - y_2) \\ \dot{y}_2 &= rx_1 - y_2 - x_1y_3, \\ \dot{y}_3 &= x_1y_2 - by_3 \end{aligned} \quad (45)$$

acoplado ao sistema mestre pela variável x_1 . De (43), obtemos:

$$\begin{aligned}\dot{e}_1 &= \sigma(e_2 - e_1) \\ \dot{e}_2 &= -e_2 - x_1 e_3. \\ \dot{e}_3 &= x_1 e_2 - b e_3\end{aligned}\quad (46)$$

Considere a função definida positiva

$$V = \frac{1}{2} \left(\frac{1}{\sigma} e_1^2 + e_2^2 + e_3^2 \right) \quad (47)$$

e sua derivada em relação ao tempo, calculada na trajetória (46)

$$\begin{aligned}\dot{V} &= \frac{1}{\sigma} e_1 \dot{e}_1 + e_2 \dot{e}_2 + e_3 \dot{e}_3, \\ \dot{V} &= \frac{1}{\sigma} e_1 \sigma(e_2 - e_1) + e_2(-e_2 - x_1 e_3) + e_3(x_1 e_2 - b e_3).\end{aligned}\quad (48)$$

A equação (48) pode ser reescrita na forma

$$\dot{V} = - \left(e_1 + \frac{e_2}{2} \right)^2 - \frac{3}{4} e_2^2 - b e_3^2. \quad (49)$$

Como V e $-\dot{V}$ são funções definidas positivas, de acordo com a teoria da estabilidade de Lyapunov, o sistema (46) é globalmente assintoticamente estável, ou seja, $e \rightarrow 0$ quando $t \rightarrow \infty$, e os sistemas (44) e (45) estão globalmente assintoticamente sincronizados.

A Figura 25 mostra o gráfico do erro de sincronização entre os sistemas mestre e escravo. O sistema em desvios é estável e o erro vai assintoticamente a zero.

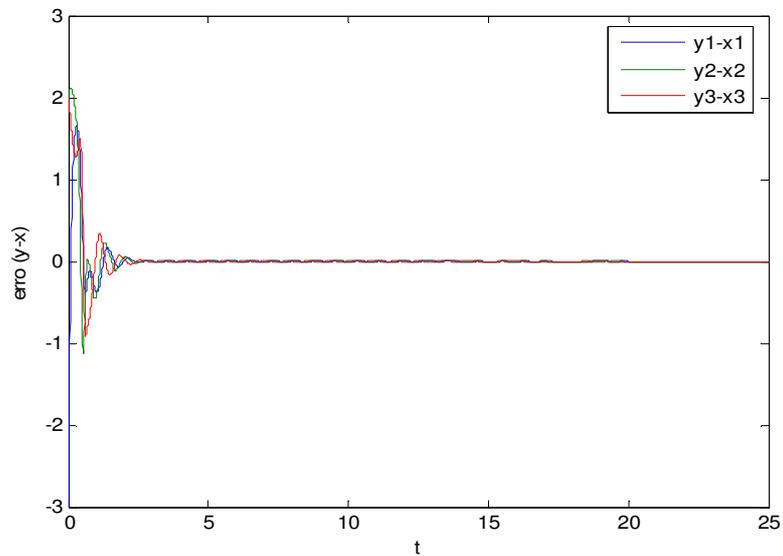


Figura 25 - Erro de sincronização dos sistemas de Lorenz acoplados

Projeto de sistema observador ([16, 30, 31, 61]). Definindo intuitivamente, um sistema observador é um sistema dinâmico que utiliza como sinal de entrada um sinal de saída de determinado sistema mestre e possui a propriedade de sua trajetória convergir para a trajetória desse sistema mestre. Uma definição precisa proposta em [31] é:

Definição 17: *Seja o sistema dinâmico*

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}), \quad (50)$$

com variável de saída $s = \mathbf{g}(\mathbf{x}) \in \mathbb{R}^n$. Dizemos que o sistema

$$\dot{\mathbf{y}} = \mathbf{f}(\mathbf{y}) + \mathbf{k}(s - \mathbf{g}(\mathbf{y})) \quad (51)$$

é um observador do sistema (50) se \mathbf{y} converge para o estado \mathbf{x} quando $t \rightarrow \infty$, onde $\mathbf{g} : \mathbb{R}^n \rightarrow \mathbb{R}^n$ é uma função não-linear apropriada. Além disso, o sistema (51) é um observador global do sistema (50) se $\mathbf{y} \rightarrow \mathbf{x}$ quando $t \rightarrow \infty$ para quaisquer condições iniciais $\mathbf{x}(0), \mathbf{y}(0)$.

O exemplo de projeto de sistema observador considerado é realizado conforme metodologia proposta em [61], baseada no conceito de observadores com dinâmica de erro

assintoticamente estável. A pergunta a ser respondida no problema da sincronização de sistemas dinâmicos através do projeto de sistemas observadores é “*dado um sistema mestre, como encontrar uma classe de possíveis sistemas observadores de forma que qualquer deles assegure a ocorrência de sincronização?*” [61].

Assim, seja um sistema mestre

$$\begin{aligned}\dot{x}_1 &= \sigma(x_2 - x_1) \\ \dot{x}_2 &= rx_1 - x_2 - x_1x_3 \\ \dot{x}_3 &= x_1x_2 - bx_3\end{aligned}\quad (52)$$

Suponha que o sistema mestre envie ao sistema escravo um sinal x_1 , ou seja:

$$h(x_1, x_2, x_3) = x_1. \quad (53)$$

Procuramos um sistema observador para (52) e (53) na forma

$$\begin{aligned}\dot{y}_1 &= \sigma(y_2 - y_1) + k_1(y_1, y_2, y_3, x_1) \\ \dot{y}_2 &= ry_1 - y_2 - y_1y_3 + k_2(y_1, y_2, y_3, x_1) \\ \dot{y}_3 &= y_1y_2 - by_3 + k_3(y_1, y_2, y_3, x_1)\end{aligned}\quad (54)$$

onde $k_i, i=1,2,3$ são funções tais que (54) é um observador para (52) e (53).

Reescrevendo o sistema em desvios, com $e = x - y$, obtemos:

$$\begin{aligned}\dot{e}_1 &= \sigma(e_2 - e_1) - k_1(y_1, y_2, y_3, x_1) \\ \dot{e}_2 &= -x_1e_3 - y_3e_1 + re_1 - e_2 - k_2(y_1, y_2, y_3, x_1) \\ \dot{e}_3 &= x_1e_2 + y_2e_1 - be_3 - k_3(y_1, y_2, y_3, x_1)\end{aligned}\quad (55)$$

Considerando a função de Lyapunov

$$V(e_1, e_2, e_3) = \frac{1}{2} \left(\frac{1}{\sigma} e_1^2 + e_2^2 + e_3^2 \right). \quad (56)$$

e sua derivada em relação do tempo, nas trajetórias (55), obtemos

$$\dot{V} = -k_1e_1 - (k_2 + y_3e_1 - (r+1)e_1)e_2 - (k_3 - y_2e_1)e_3 - e_1^2 - e_2^2 - be_3^2. \quad (57)$$

Se as funções k_1, k_2 e k_3 satisfazem a desigualdade $\dot{V} < 0$ para $e_1, e_2, e_3 \neq 0$, sabemos, pela teoria da estabilidade de Lyapunov, que $e_1(t), e_2(t), e_3(t) \rightarrow 0$ quando $t \rightarrow \infty$.

Assim, tomando

$$\begin{aligned}
k_1(y_1, y_2, y_3, x_1) &= 0 \\
k_2(y_1, y_2, y_3, x_1) &= -y_3(x_1 - y_1) + (r+1)(x_1 - y_1) \\
k_3(y_1, y_2, y_3, x_1) &= y_2(x_1 - y_1)
\end{aligned} \tag{58}$$

e levando (58) em (57), obtemos:

$$\dot{V} = -e_1^2 - e_2^2 - be_3^2. \tag{59}$$

Portanto, como V e $-\dot{V}$ são funções definidas positivas, de acordo com a teoria da estabilidade de Lyapunov, o sistema (46) é globalmente assintoticamente estável, ou seja, $e \rightarrow 0$ quando $t \rightarrow \infty$, e os sistemas estão globalmente sincronizados, ou seja, o sistema observador (54) reconstrói assintoticamente as variáveis de estado do sistema mestre (52).

A Figura 26 apresenta o gráfico do erro de sincronização dos sistemas mestre e escravo.

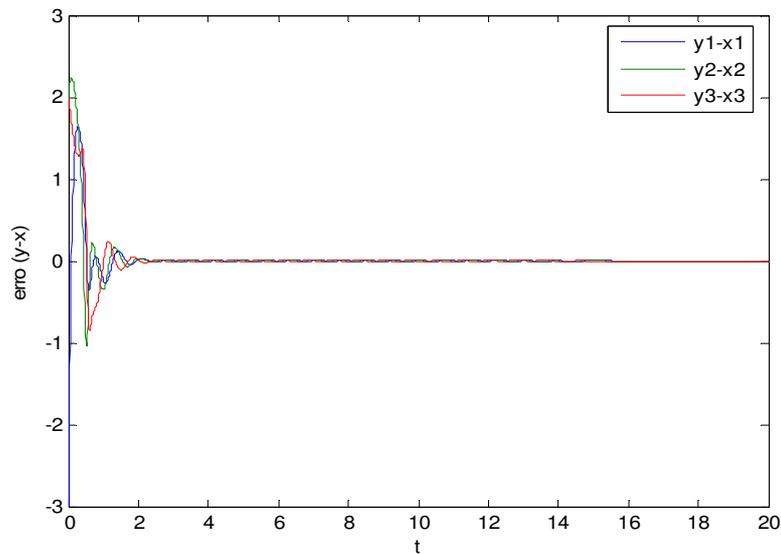


Figura 26 - Erro de sincronização dos sistemas de Lorenz com observador

Controle Mestre-Escravo ([35]). Sejam os sistemas mestre (60) e escravo (61)

$$\dot{x} = f(x) \tag{60}$$

$$\dot{y} = f(y, u) \tag{61}$$

onde

$$\dot{e} = \dot{y} - \dot{x} \tag{62}$$

é o sistema em desvios. Definindo uma função de controle \mathbf{u} tal que

$$\dot{\mathbf{e}} = -\mathbf{e} \quad (63)$$

o estado \mathbf{y} converge para o estado \mathbf{x} quando $t \rightarrow \infty$, onde $\mathbf{u}: \mathbb{R}^n \rightarrow \mathbb{R}^n$ é uma função apropriada. Além disso, se $\mathbf{y} \rightarrow \mathbf{x}$ quando $t \rightarrow \infty$ para quaisquer condições iniciais $\mathbf{x}(0)$, $\mathbf{y}(0)$, dizemos que o sistema (62) é globalmente assintoticamente estável.

Seja o sistema mestre:

$$\begin{aligned} \dot{x}_1 &= -\sigma(x_1 - x_2) \\ \dot{x}_2 &= rx_1 - x_2 - x_1x_3 \cdot \\ \dot{x}_3 &= x_1x_2 - bx_3 \end{aligned} \quad (64)$$

Seja o sistema escravo com controle

$$\begin{aligned} \dot{y}_1 &= \sigma(y_2 - y_1) + u_1 \\ \dot{y}_2 &= ry_1 - y_2 - y_1y_3 + u_2 \cdot \\ \dot{y}_3 &= y_1y_2 - by_3 + u_3 \end{aligned} \quad (65)$$

Definindo o vetor erro como

$$\mathbf{e} = \mathbf{y} - \mathbf{x} \quad (66)$$

obtemos o sistema em desvios

$$\begin{aligned} \dot{e}_1 &= \sigma(e_2 - e_1) + u_1 \\ \dot{e}_2 &= re_1 - e_2 + x_1x_3 - y_1y_3 + u_2 \cdot \\ \dot{e}_3 &= y_1y_2 - x_1x_2 - be_3 + u_3 \end{aligned} \quad (67)$$

Considerando-se a equação (63), definimos a função de controle \mathbf{u} como

$$\mathbf{u} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} e_1(\sigma - 1) - \sigma e_2 \\ -re_1 - x_1x_3 + y_1y_3 \\ e_3(b - 1) - y_1y_2 + x_1x_2 \end{pmatrix}. \quad (68)$$

E, finalmente, o sistema em desvios pode ser reescrito como

$$\dot{\mathbf{e}} = \begin{pmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \end{pmatrix} = - \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix}. \quad (69)$$

Escolhendo uma função de Lyapunov na forma

$$V = \frac{1}{2}(e_1^2 + e_2^2 + e_3^2) \quad (70)$$

e calculando sua derivada em relação ao tempo na trajetória (69), obtemos:

$$\dot{V} = -(e_1^2 + e_2^2 + e_3^2). \quad (71)$$

De acordo com a teoria da estabilidade de Lyapunov, o sistema em desvios é globalmente assintoticamente estável e $\|e\| = \|y - x\| \rightarrow 0$ quando $t \rightarrow \infty$, e os sistemas estão globalmente assintoticamente sincronizados.

A Figura 27 apresenta o gráfico do erro de sincronização dos sistemas com controle mestre-escravo.

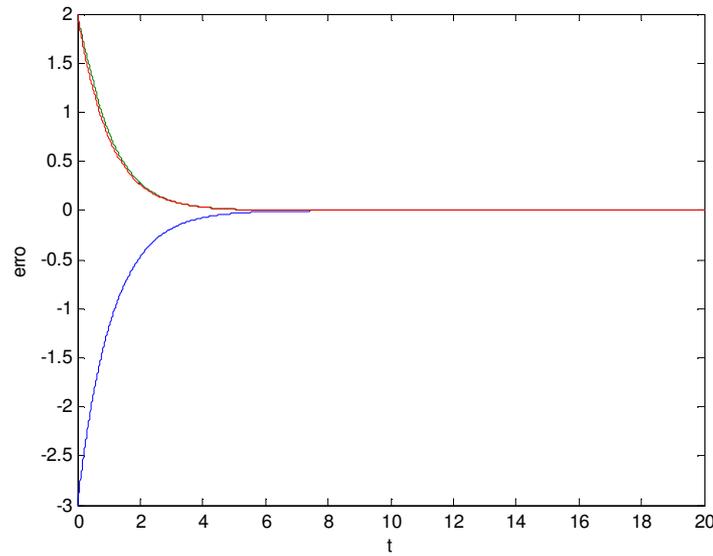


Figura 27 - Erro de sincronização dos sistemas de Lorenz com Controle mestre-escravo

Controle Não-Linear ([24, 25]). Sejam os sistemas caóticos mestre (72) e escravo (73) descritos pelas equações

$$\dot{x} = A_1 x + f_1(x) \quad (72)$$

$$\dot{y} = A_2 y + f_2(y) + U \quad (73)$$

onde $x, y \in R^n$ são vetores de estado dos sistemas, $A_1, A_2 \in R^{n \times n}$ é a matriz de parâmetros dos termos lineares, $f_1, f_2 : R^n \rightarrow R^n$ são vetores de funções não-lineares e $u \in R^n$ é o vetor de das funções de controle. Se $A_1 = A_2$ e $f_1 = f_2$, então x e y representam o estado de dois sistemas caóticos idênticos; caso contrário, se $A_1 \neq A_2$ ou $f_1 \neq f_2$, x e y representam o estado de dois sistemas caóticos diferentes.

Subtraindo (72) de (73), obtemos o sistema em desvios $\dot{e} = \dot{y} - \dot{x}$, ou seja,

$$\dot{\mathbf{e}} = A_2 \mathbf{y} + \mathbf{f}_2(\mathbf{y}) - A_1 \mathbf{x} - \mathbf{f}_1(\mathbf{x}) + \mathbf{u} \quad (74)$$

Assim, o problema da sincronização se reduz a encontrar o controle \mathbf{u} que estabiliza o sistema em desvios (74) na origem.

Seja o sistema mestre:

$$\begin{aligned} \dot{x}_1 &= -\sigma(x_1 - x_2) \\ \dot{x}_2 &= rx_1 - x_2 - x_1x_3 \\ \dot{x}_3 &= x_1x_2 - bx_3 \end{aligned} \quad (75)$$

Seja o sistema escravo com controle

$$\begin{aligned} \dot{y}_1 &= \sigma(y_2 - y_1) + u_1 \\ \dot{y}_2 &= ry_1 - y_2 - y_1y_3 + u_2 \\ \dot{y}_3 &= y_1y_2 - by_3 + u_3 \end{aligned} \quad (76)$$

Subtraindo (75) de (76) obtemos o sistema em desvios

$$\begin{aligned} \dot{e}_1 &= \sigma(e_2 - e_1) + u_1 \\ \dot{e}_2 &= re_1 - e_2 + x_1x_3 - y_1y_3 + u_2 \\ \dot{e}_3 &= y_1y_2 - x_1x_2 - be_3 + u_3 \end{aligned} \quad (77)$$

Escolhendo uma função de Lyapunov e calculando sua derivada em relação ao tempo, temos

$$V = \mathbf{e}^T P \mathbf{e} \quad (78)$$

$$\dot{V} = \dot{\mathbf{e}}^T P \mathbf{e} + \mathbf{e}^T P \dot{\mathbf{e}} \quad (79)$$

onde P é uma matriz definida positiva. A seguir, é necessário encontrar a função de controle \mathbf{u} tal que a derivada de (78) em relação ao tempo na trajetória (77) seja uma função definida negativa. Escolhendo

$$\mathbf{u} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} -\sigma e_2 \\ -re_1 + y_1y_3 - x_1x_3 \\ x_1x_2 - y_1y_2 \end{pmatrix}; \quad P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad (80)$$

Levando (80) em (79), obtemos

$$\dot{V} = \begin{pmatrix} e_1 & e_2 & e_3 \end{pmatrix} \begin{pmatrix} -\sigma & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -b \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix}$$

De acordo com a teoria da estabilidade de Lyapunov, os sistemas mestre e escravo estão globalmente assintoticamente sincronizados, e $\lim_{t \rightarrow \infty} \|e(t)\| \rightarrow 0$. A Figura 28 apresenta o gráfico do erro de sincronização dos sistemas.

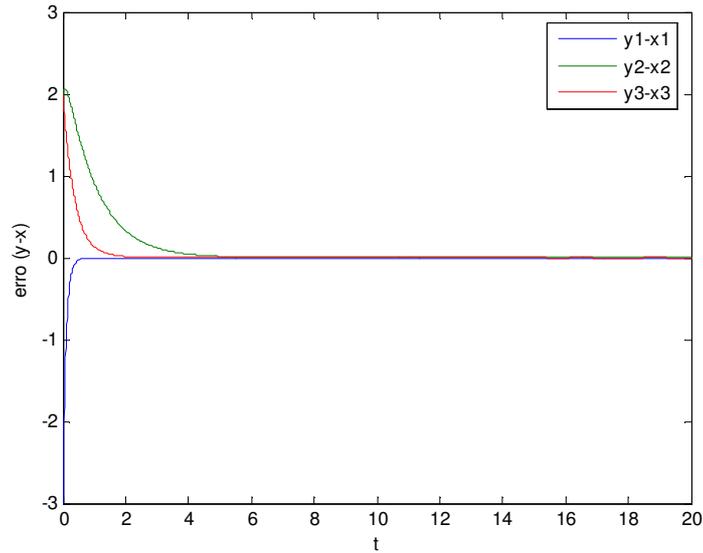


Figura 28 - Erro de sincronização do sistema de Lorenz via controle não-linear

Controle Ativo ([79]) Sejam os sistemas caóticos mestre (81) e escravo (82) descritos pelas equações

$$\dot{x} = A_1 x + f_1(x) \quad (81)$$

$$\dot{y} = A_2 y + f_2(y) + u \quad (82)$$

onde $x, y \in \mathbb{R}^n$ são vetores de estado dos sistemas, $A_1, A_2 \in \mathbb{R}^{n \times n}$ é a matriz de parâmetros dos termos lineares, $f_1, f_2: \mathbb{R}^n \rightarrow \mathbb{R}^n$ são vetores de funções não-lineares e $u \in \mathbb{R}^n$ é o vetor de das funções de controle. Se $A_1 = A_2$ e $f_1 = f_2$, então x e y representam o estado de dois sistemas caóticos idênticos; caso contrário, se $A_1 \neq A_2$ ou $f_1 \neq f_2$, x e y representam o estado de dois sistemas caóticos diferentes.

Subtraindo (81) de (82), obtemos o sistema em desvios $\dot{e} = \dot{y} - \dot{x}$, ou seja,

$$\dot{e} = A_2 y + f_2(y) - A_1 x - f_1(x) + u \quad (83)$$

Assim, o problema da sincronização se reduz a encontrar o controle u que estabiliza o sistema em desvios (83) na origem.

Para ilustrar o funcionamento do controle ativo, apresentamos a seguir a sincronização dos sistemas de Chen (mestre) e Lorenz (escravo).

Seja o sistema mestre

$$\begin{aligned}\dot{x}_1 &= a(x_2 - x_1) \\ \dot{x}_2 &= cx_2 - x_1x_3 . \\ \dot{x}_3 &= x_1x_2 - bx_3\end{aligned}\tag{84}$$

Seja o sistema escravo

$$\begin{aligned}\dot{y}_1 &= \sigma(y_2 - y_1) + u_1 \\ \dot{y}_2 &= ry_1 - y_2 - y_1y_3 + u_2 . \\ \dot{y}_3 &= y_1y_2 - \beta y_3 + u_3\end{aligned}\tag{85}$$

Subtraindo (84) de (85) e denotando $e = y - x$, obtemos o sistema em desvios

$$\begin{aligned}\dot{e}_1 &= \alpha(e_2 - e_1) + (\alpha - a)(x_2 - x_1) + u_1 \\ \dot{e}_2 &= ry_1 - e_2 - y_1e_3 - x_3e_1 - (c + 1)x_2 + u_2 . \\ \dot{e}_3 &= y_1e_2 + x_2e_1 - \beta e_3 + (-\beta + b)x_3 + u_3\end{aligned}\tag{86}$$

Definimos as funções de controle ativo como

$$\begin{aligned}u_1(t) &= W_1(t) - (\alpha - a)(x_2 - x_1) \\ u_2(t) &= W_2(t) - ry_1 + y_1e_3 + x_3e_1 + (c + 1)x_2 , \\ u_3(t) &= W_3(t) - y_1e_2 - x_2e_1 + (\beta - b)x_3\end{aligned}\tag{87}$$

o sistema em desvios pode ser escrito em forma linear

$$\begin{pmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \end{pmatrix} = \begin{pmatrix} -\alpha & \alpha & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -\beta \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} + \begin{pmatrix} W_1(t) \\ W_2(t) \\ W_3(t) \end{pmatrix}\tag{88}$$

onde as funções $W_1(t), W_2(t), W_3(t)$ são entradas de sinal de controle como função dos desvios e_1, e_2, e_3 . Se esses sinais de controle estabilizam o sistema em desvios (88), então

$\|(e_1, e_2, e_3)\| \rightarrow 0$ quando $t \rightarrow \infty$, e os sistemas (84) e (85) estão sincronizados.

Escolhemos

$$\begin{pmatrix} W_1(t) \\ W_2(t) \\ W_3(t) \end{pmatrix} = A \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix}\tag{89}$$

onde $A_{3 \times 3}$ é uma matriz constante. Para que o sistema com realimentação seja estável, é preciso escolher a matriz A de forma que todos os autovalores de (88) tenham parte real negativa.

Escolhemos

$$A = \begin{pmatrix} \alpha & -\alpha & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \beta - 1 \end{pmatrix}. \quad (90)$$

E dessa forma o sistema (88) se torna

$$\begin{pmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \end{pmatrix} = \begin{pmatrix} -e_1 \\ -e_2 \\ -e_3 \end{pmatrix}, \quad (91)$$

ou simplesmente

$$\dot{e} = -e \quad (92)$$

e tem autovalores $\lambda_1 = \lambda_2 = \lambda_3 = -1$. Pela teoria da estabilidade de sistemas lineares, o sistema é globalmente assintoticamente estável.

Para provar a estabilidade, escolhemos uma função de Lyapunov na forma

$$V = \frac{1}{2}(e_1^2 + e_2^2 + e_3^2), \quad (93)$$

cuja derivada em relação ao tempo é

$$\dot{V} = \dot{e}_1 e_1 + \dot{e}_2 e_2 + \dot{e}_3 e_3. \quad (94)$$

Calculando o valor de (94) na trajetória (92), obtemos

$$\dot{V} = -e_1^2 - e_2^2 - e_3^2. \quad (95)$$

Segundo a teoria da estabilidade de Lyapunov, como V e $-\dot{V}$ são funções definidas positivas, então a origem do sistema (92) é um ponto assintoticamente estável. A Figura 29 apresenta o gráfico do erro de sincronização.

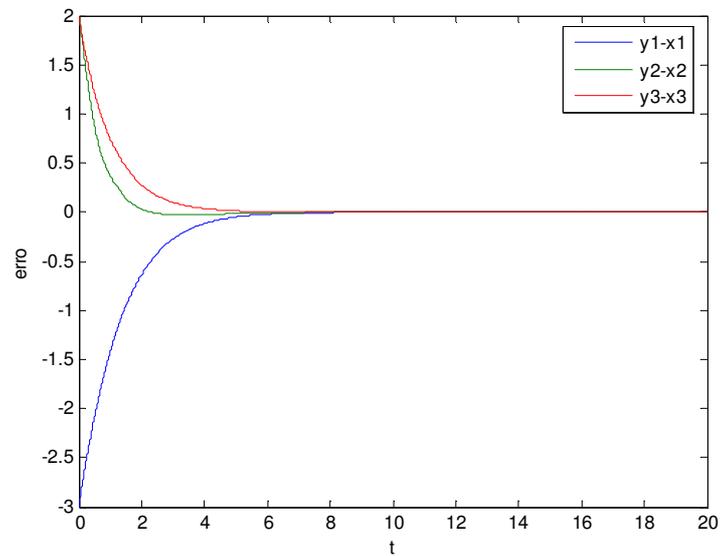


Figura 29 - Erro de sincronização sistemas de Chen e Lorenz - controle ativo

3.5 Considerações finais

Apresentamos neste capítulo cinco enfoques diferentes a partir dos quais a sincronização de caos pode ser abordada. Assim, partindo desse estudo, torna-se possível apreciar esses enfoques quanto aos seus pontos fracos e fortes, tendo em vista a aplicação em comunicação.

Do ponto de vista geral, determinado enfoque pode ser preferido à outro, dependendo dos critérios e objetivos de cada pesquisa. No caso desta pesquisa, a facilidade de implementação e o tempo gasto na sincronização são especialmente desejáveis.

A sincronização por acoplamento é possível em alguns casos, e isso depende da variável acoplada e da forma do acoplamento.

Existem casos quando é difícil encontrar uma função de Lyapunov apropriada para estudar a estabilidade de forma analítica e essa característica é comum a todos os enfoques de sincronização de caos estudados no capítulo. Além disso, em muitos casos, a sincronização de sistemas acoplados fica restrita a determinados intervalos de valores dos seus parâmetros [50], o que se torna um fator limitante na aplicação em comunicação segura.

Nas metodologias de controle mestre-escravo, de controle não-linear e de controle ativo, o sistema em desvios pode ser conduzido assintoticamente a zero e isso depende da forma como a função de controle u é escolhida. Isso significa que os métodos são globalmente assintoticamente estáveis, desde que uma função de controle apropriada seja escolhida. Em contrapartida, um inconveniente dessas metodologias é que, em geral, a função de controle escolhida u necessita de considerável volume de informações a respeito do estado atual do sistema.

Além disso, esses enfoques estabilizam os sistemas em desvios anulando termos indesejáveis e não-lineares presentes nesses sistemas e acrescentando termos desejáveis, de forma a obter uma função \dot{V} definida negativa cujos termos também sejam negativos definidos.

O mesmo ocorre no projeto de um sistema observador, onde a função k cumpre papel semelhante ao da função de controle das demais metodologias. Dessa forma, esses métodos perdem em generalidade. Para um novo sistema, o problema da sincronização deve ser reformulado e novamente resolvido. Além disso, um problema de sincronização de sistemas diferentes, como proposto em [79] é, em última análise, transformado em um problema de sincronização de sistemas iguais, já que os termos que não são comuns aos dois sistemas são simplesmente eliminados pela função de controle.

A eliminação das não-linearidades também torna as metodologias citadas menos atraentes do ponto de vista da aplicação em comunicação segura pois a riqueza da dinâmica dos sistemas é justamente resultado da existência de termos não-lineares.

Considerando a inexistência de uma maneira sistemática de encontrar funções de Lyapunov apropriadas para sistemas não-lineares, a resolução de um problema de sincronização através dos métodos apresentados neste capítulo pode se tornar uma tarefa demorada, infrutífera e enfadonha.

Dentre os enfoques estudados, os melhores desempenhos com relação ao tempo gasto na tarefa de sincronização mostram a estabilização do sistema em desvios após decorridos aproximadamente 3 segundos de desempenho dos sistemas.

4 SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS VIA CONTROLE ÓTIMO LINEAR FEEDBACK

4.1 Introdução

O controle *feedback*, também conhecido como controle com *realimentação*, *retroalimentação* ou *em malha fechada*, é um mecanismo matemático que regula e estabiliza o comportamento de sistemas dinâmicos. O termo *feedback* deve-se ao fato de que o sinal de controle é função da diferença entre valores atuais e valores desejados das variáveis de estado do sistema, de forma que o controle utiliza a saída do sistema para *realimentá-lo* através do sinal de controle.

A metodologia do controle *ótimo* busca controlar o processo da forma desejada ao mesmo tempo em que minimiza um índice de desempenho. Como exemplo pode-se considerar um jato que propuliona um satélite à órbita desejada de forma a minimizar o consumo de combustível.

Em se tratando de sincronização, a trajetória desejada de um sistema *escravo* é a trajetória de um sistema *mestre*, e o sinal de controle (a realimentação) em determinado instante é função da diferença entre as trajetórias no instante anterior.

A teoria do controle linear feedback, originalmente desenvolvida para aplicação em sistemas lineares, pode ser estendida para controle e sincronização de sistemas não-lineares, inclusive sistemas que apresentam dinâmica caótica [17, 37, 64]. Nesse caso o problema se torna ainda mais interessante porque sistemas caóticos amplificam exponencialmente quaisquer perturbações a que são submetidos, e quaisquer erros arbitrariamente pequenos entre as trajetórias tendem a crescer exponencialmente até tornarem-se da ordem da amplitude da própria dinâmica do sistema. Dessa forma, em se tratando de simulações computacionais, para garantir que a sincronização se sustente na ausência de controle, é necessário que o nível de exatidão das trajetórias seja da ordem da própria capacidade de cálculo da máquina.

O presente capítulo apresenta a metodologia do controle ótimo linear feedback para sistemas não-lineares, conforme proposto em [64].

4.2 Regulador ótimo linear com funcional quadrático

Seja o sistema dinâmico linear

$$\dot{\mathbf{x}}(t) = A(t)\mathbf{x}(t) + B(t)\mathbf{u}(t) \quad (96)$$

com condições iniciais

$$\mathbf{x}(0) = \mathbf{x}_0 \quad (97)$$

onde $\mathbf{x} \in R^n$ é o vetor de estados, $A \in R^{n \times n}$ e $B \in R^{n \times m}$ são matrizes e $\mathbf{u} \in R^m$ é o vetor de controle que minimiza o funcional

$$J = \int_0^{t_f} [\mathbf{x}^T(t)Q(t)\mathbf{x}(t) + \mathbf{u}^T(t)R(t)\mathbf{u}(t)] dt. \quad (98)$$

No caso de t_f finito, todas as matrizes envolvidas no problema podem depender do tempo e diz-se que o problema é de “horizonte finito”. No caso de t_f infinito, todas as matrizes são constantes, e diz-se que o problema é de “horizonte infinito” [43, 55].

Considere uma função de Lyapunov na forma

$$V(\mathbf{x}, t) = \mathbf{x}^T P(t)\mathbf{x} \quad (99)$$

e considere, da teoria da programação dinâmica, a equação de *Hamilton-Jacobi-Bellman*

$$\min_{\mathbf{u}(t)} \left[\frac{dV}{dt} + (\text{grad}V)^T (A(t)\mathbf{x} + B(t)\mathbf{u}) + \mathbf{x}^T Q(t)\mathbf{x} + \mathbf{u}^T R(t)\mathbf{u} \right] = 0 \quad (100)$$

onde $\text{grad}V = \left(\frac{\partial V}{\partial x_1} \quad \frac{\partial V}{\partial x_2} \quad \dots \quad \frac{\partial V}{\partial x_n} \right)^T$. A solução da equação de Hamilton-Jacobi-

Bellman é procurada em forma da função (99), onde $P(t)$ é matriz a determinar. Admitindo que $\text{grad}V = 2P(t)\mathbf{x}$, da condição do mínimo de (100), obtemos o controle ótimo

$$\mathbf{u} = -R^{-1}(t)B^T(t)P(t)\mathbf{x}. \quad (101)$$

Levando (101) em (100) e admitindo $P(t)$ simétrica, obtém-se:

$$\mathbf{x}^T \left[\frac{dP(t)}{dt} + 2A(t) - 2P(t)B(t)R^{-1}(t)B^T(t)P(t) + Q(t) + P(t)B(t)R^{-1}(t)B^T(t)P(t) \right] \mathbf{x} = 0 \quad (102)$$

Como o vetor de estados \mathbf{x} assume valores diferentes de zero, resta que

$$\dot{P} + A^T P + PA - PBR^{-1}B^T P + Q = 0. \quad (103)$$

Por definição, $V(\mathbf{x}, t_f) = 0$, então obtemos a condição final

$$P(t_f) = 0. \quad (104)$$

Para sistemas autônomos, as matrizes A , B , Q e R são constantes e as equações (96), (98), (99) e (103) tornam-se, respectivamente (105), (106), (107) e (108)

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{u}(t) \quad (105)$$

$$J = \int_0^{\infty} [\mathbf{x}^T(t)Q\mathbf{x}(t) + \mathbf{u}^T(t)R\mathbf{u}(t)] dt \quad (106)$$

$$V = \mathbf{x}^T P \mathbf{x} \quad (107)$$

$$A^T P + PA - PBR^{-1}B^T P + Q = 0. \quad (108)$$

Nesse caso, a lei de controle

$$\mathbf{u} = -R^{-1}B^T P \mathbf{x} \quad (109)$$

fornece mínimo ao funcional (106), calculado nas trajetórias ótimas do sistema (105). A estabilidade assintótica do sistema (105) é assegurada através da positividade definida das matrizes Q e R .

A condição suficiente para que o valor do funcional (106) seja finito, ou seja, para que o sistema (105) seja assintoticamente estável, é a controlabilidade completa das matrizes A e B [55]; para que as matrizes sejam completamente controláveis, a matriz de controlabilidade

$$\begin{pmatrix} B & AB & \dots & A^{n-1}B \end{pmatrix} \quad (110)$$

deve ter posto n , ou seja, ter n colunas linearmente independentes. Nesse caso

$$\text{rank} \begin{pmatrix} B & AB & \dots & A^{n-1}B \end{pmatrix} = n. \quad (111)$$

4.3 Sincronização de sistemas não-lineares via controle ótimo linear feedback

Nesta seção o problema do controle ótimo de sistemas não-lineares é formulado e resolvido para a sincronização de sistemas caóticos. O problema do controle ótimo de sistemas caóticos é anterior ao problema da sincronização, e difere deste no sentido de que o controle procura estabilizar a trajetória do sistema em uma órbita ou ponto desejado, enquanto a sincronização busca levar a trajetória de um sistema (escravo) à de outro (mestre).

Considere o sistema mestre (112) e o sistema escravo (113)

$$\dot{\mathbf{x}} = A\mathbf{x} + \mathbf{g}(\mathbf{x}) \quad (112)$$

$$\dot{\mathbf{y}} = A\mathbf{y} + \mathbf{g}(\mathbf{y}) + B\mathbf{u} \quad (113)$$

sujeitos a

$$\mathbf{x}(0) = \mathbf{x}_0 \quad (114)$$

$$\mathbf{y}(0) = \mathbf{y}_0 \quad (115)$$

onde $\mathbf{x}, \mathbf{y} \in R^n$ são vetores de estado; $A \in R^{n \times n}$ é a matriz dos termos lineares; $\mathbf{g}(\cdot)$ é o vetor das funções não-lineares, $B \in R^{n \times m}$ é uma matriz constante e $\mathbf{u} \in R^m$ é um vetor de controle que estabiliza o sistema escravo na trajetória desejada.

Podemos definir o vetor erro como

$$\mathbf{e} = \mathbf{y} - \mathbf{x}. \quad (116)$$

E obtemos o sistema em desvios

$$\begin{aligned} \dot{\mathbf{e}} &= A\mathbf{e} + \mathbf{g}(\mathbf{y}) - \mathbf{g}(\mathbf{x}) + B\mathbf{u} \\ &= A\mathbf{e} + \mathbf{g}(\mathbf{x} + \mathbf{e}) - \mathbf{g}(\mathbf{x}) + B\mathbf{u}. \end{aligned} \quad (117)$$

Introduzindo

$$\mathbf{h}(\mathbf{x}, \mathbf{e}) = \mathbf{g}(\mathbf{x} + \mathbf{e}) - \mathbf{g}(\mathbf{x}), \quad (118)$$

obtemos

$$\dot{\mathbf{e}} = A\mathbf{e} + \mathbf{h}(\mathbf{x}, \mathbf{e}) + B\mathbf{u}. \quad (119)$$

Teorema 8: *Se existem matrizes Q e R , definidas positivas, sendo Q simétrica, de forma que a função*

$$l(\mathbf{x}, \mathbf{e}) = \mathbf{e}^T Q \mathbf{e} - \mathbf{h}^T(\mathbf{x}, \mathbf{e}) P \mathbf{e} - \mathbf{e}^T P \mathbf{h}(\mathbf{x}, \mathbf{e}) \quad (120)$$

é definida positiva, onde a matriz P é a solução da seguinte equação algébrica matricial de Riccati

$$PA + A^T P - PBR^{-1}B^T P + Q = 0 \quad (121)$$

então, o controle linear feedback

$$\mathbf{u} = -R^{-1}B^T P \mathbf{e} \quad (122)$$

é ótimo no sentido de transferir o sistema em desvios (119) de qualquer estado inicial ao estado final

$$\lim_{t \rightarrow \infty} \mathbf{e}(t) = 0 \quad (123)$$

minimizando o funcional

$$J = \int_0^{\infty} [l(\mathbf{x}, \mathbf{e}) + \mathbf{u}^T R \mathbf{u}] dt. \quad (124)$$

Se a condição suficiente $l(\mathbf{x}, \mathbf{e}) \geq 0, \forall \mathbf{e}(t) \in \mathbb{R}^n$ é satisfeita, o sistema em desvios (119) é globalmente assintoticamente estável, e isso implica que o sistema mestre e o sistema escravo estão globalmente assintoticamente sincronizados.

Prova. Considere o controle ótimo feedback (122), com matriz P determinada pela equação (121), que transfere o sistema não-linear (119) de um estado inicial para o estado final (123) minimizando o funcional (124) onde a função $l(\mathbf{x}, \mathbf{e})$ precisa ser determinada.

De acordo com as regras da programação dinâmica, se o mínimo do funcional (124) existe, e se V é uma função suave das condições iniciais, então ela satisfaz a equação de *Hamilton-Jacobi-Bellman*:

$$\min \left(\frac{dV}{dt} + \mathbf{e}^T l(\mathbf{x}, \mathbf{e}) \mathbf{e} + \mathbf{u}^T R \mathbf{u} \right) = 0. \quad (125)$$

Considerando a função de Lyapunov

$$V = \mathbf{e}^T P \mathbf{e} \quad (126)$$

onde P é uma matriz simétrica definida positiva e satisfaz a equação algébrica matricial de Ricatti (121).

Note que a derivada da função V , quando avaliada na trajetória ótima com controle, é

$$\begin{aligned}
\dot{V} &= \dot{\mathbf{e}}^T P \mathbf{e} + \mathbf{e}^T P \dot{\mathbf{e}} \\
&= (\mathbf{A} \mathbf{e} + \mathbf{h}(\mathbf{x}, \mathbf{e}) + \mathbf{B} \mathbf{u})^T P \mathbf{e} + \mathbf{e}^T P (\mathbf{A} \mathbf{e} + \mathbf{h}(\mathbf{x}, \mathbf{e}) + \mathbf{B} \mathbf{u}) \\
&= \mathbf{e}^T \mathbf{A}^T P \mathbf{e} + \mathbf{h}^T(\mathbf{x}, \mathbf{e}) P \mathbf{e} + \mathbf{u}^T \mathbf{B}^T P \mathbf{e} + \mathbf{e}^T P \mathbf{A} \mathbf{e} + \mathbf{e}^T P \mathbf{h}(\mathbf{x}, \mathbf{e}) + \mathbf{e}^T P \mathbf{B} \mathbf{u} \\
&= \mathbf{e}^T \mathbf{A}^T P \mathbf{e} + \mathbf{h}^T(\mathbf{x}, \mathbf{e}) P \mathbf{e} + \mathbf{e}^T P \mathbf{A} \mathbf{e} + \mathbf{e}^T P \mathbf{h}(\mathbf{x}, \mathbf{e}) - \mathbf{e}^T P \mathbf{B} \mathbf{R}^{-1} \mathbf{B}^T P \mathbf{e} - \mathbf{e}^T P \mathbf{B} (\mathbf{R}^{-1})^T \mathbf{B}^T P \mathbf{e}.
\end{aligned} \tag{127}$$

Substituindo \dot{V} na equação de *Hamilton-Jacobi-Bellman* (125), obtemos:

$$\begin{aligned}
\mathbf{e}^T (\mathbf{A}^T P + P \mathbf{A} - P \mathbf{B} \mathbf{R}^{-1} \mathbf{B}^T P) \mathbf{e} + \mathbf{h}^T(\mathbf{x}, \mathbf{e}) P \mathbf{e} + \mathbf{e}^T P \mathbf{h}(\mathbf{x}, \mathbf{e}) + l(\mathbf{x}, \mathbf{e}) &= 0 \\
\mathbf{e}^T (\mathbf{A}^T P + P \mathbf{A} - P \mathbf{B} \mathbf{R}^{-1} \mathbf{B}^T P + Q) \mathbf{e} - \mathbf{e}^T Q \mathbf{e} + \mathbf{h}^T(\mathbf{x}, \mathbf{e}) P \mathbf{e} + \mathbf{e}^T P \mathbf{h}(\mathbf{x}, \mathbf{e}) + l(\mathbf{x}, \mathbf{e}) &= 0
\end{aligned}$$

e, finalmente

$$l(\mathbf{x}, \mathbf{e}) = \mathbf{e}^T Q \mathbf{e} - \mathbf{h}^T(\mathbf{x}, \mathbf{e}) P \mathbf{e} - \mathbf{e}^T P \mathbf{h}(\mathbf{x}, \mathbf{e}). \tag{128}$$

Observe que para uma função definida positiva $l(\mathbf{x}, \mathbf{e})$ e uma matriz definida positiva R , a derivada da função (126), avaliada na trajetória ótima do sistema (119), é dada por $\dot{V} = -l(\mathbf{x}, \mathbf{e}) - \mathbf{u}^T R \mathbf{u}$, e é definida negativa. Então a função (126) é uma função de Lyapunov, e de acordo com a teoria da estabilidade de Lyapunov, podemos concluir que o sistema em desvios (119) é globalmente assintoticamente estável se a função (120) é definida positiva para qualquer $\mathbf{e} \in R^n$. Portanto, o sistema mestre (112) e o sistema escravo (113), controlado por (122), estão globalmente assintoticamente sincronizados. De acordo com a teoria do controle ótimo de sistemas lineares com funcional quadrático (124), a solução da equação algébrica matricial de Riccati (122) é uma matriz definida positiva e simétrica $P > 0$ para quaisquer $R > 0$ e $Q > 0$ dados, e assim a prova do teorema está completa.

4.4 Simulações numéricas

São apresentadas a seguir as simulações da sincronização dos sistemas de Lorenz, Chen e Lü através do controle ótimo linear feedback, para os valores de parâmetros originais dos sistemas. As simulações numéricas foram realizadas com o

método de Runge-Kutta de 4ª ordem, com passo de integração $h=10^{-2}$ e condições

$$\text{iniciais, } \mathbf{x}(\mathbf{0}) = \begin{pmatrix} -20 \\ 10 \\ 30 \end{pmatrix} \text{ e } \mathbf{y}(\mathbf{0}) = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}.$$

Sincronização do sistema de Lorenz. Podemos escrever os sistemas mestre (129) e escravo (130) na forma matricial

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{pmatrix} = \begin{pmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -8/3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{pmatrix}, \quad (129)$$

$$\begin{pmatrix} \dot{y}_1 \\ \dot{y}_2 \\ \dot{y}_3 \end{pmatrix} = \begin{pmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -8/3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} 0 \\ -y_1 y_3 \\ y_1 y_2 \end{pmatrix} + \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}. \quad (130)$$

Escolhendo

$$Q = B = R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (131)$$

considerando a matriz

$$A = \begin{pmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -8/3 \end{pmatrix} \quad (132)$$

e resolvendo a equação algébrica não-linear de Ricatti através do comando *lqr* do software MATLAB®, obtemos a função de controle:

$$\mathbf{u} = - \begin{pmatrix} 14,7479 & 11,4912 & 0 \\ 11,4912 & 8,9888 & 0 \\ 0 & 0 & 0,1813 \end{pmatrix} \begin{pmatrix} y_1 - x_1 \\ y_2 - x_2 \\ y_3 - x_3 \end{pmatrix}. \quad (133)$$

A Figura 30, a Figura 31 e a Figura 32 mostram o resultado da simulação para o sistema de Lorenz.

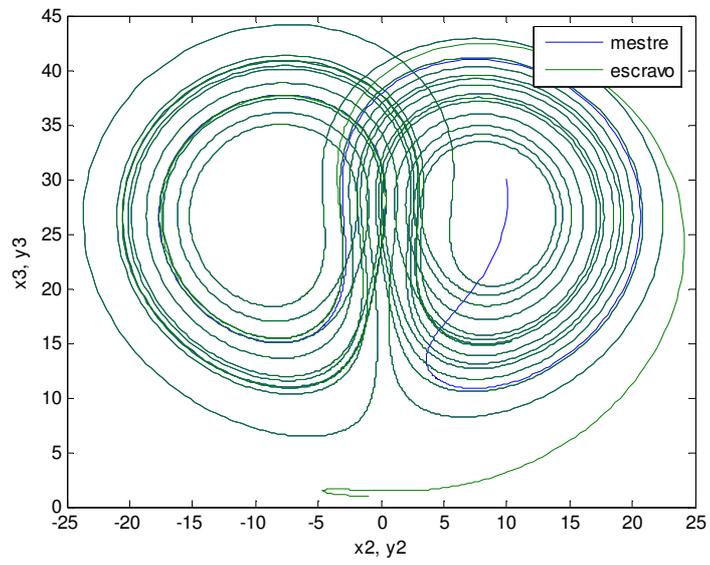


Figura 30 - Dinâmica dos sistemas de Lorenz em 2D

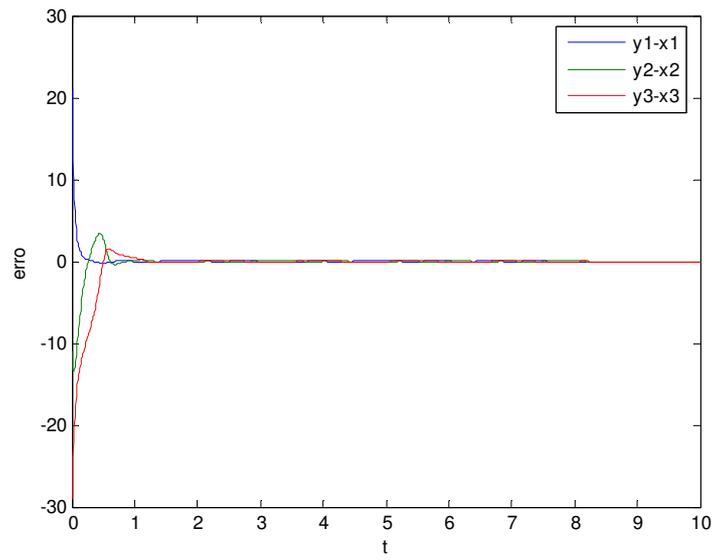


Figura 31 - Erro de sincronização - Sistema de Lorenz

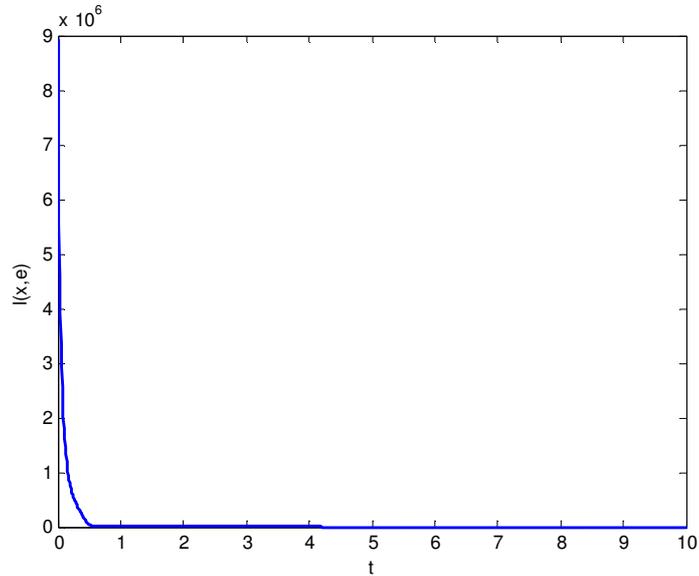


Figura 32 - Avaliação da função $l(x,e)$ – Sistema de Lorenz

Considerando a teoria da estabilidade de Lyapunov, a avaliação da função $l(x,e)$, definida positiva na trajetória, mostra que o controle aplicado é ótimo e assintoticamente estável.

Sincronização do sistema de Chen. Escrevendo os sistemas mestre (134) e escravo (135) na forma matricial

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{pmatrix} = \begin{pmatrix} -35 & 35 & 0 \\ -7 & 28 & 0 \\ 0 & 0 & -3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{pmatrix}, \quad (134)$$

$$\begin{pmatrix} \dot{y}_1 \\ \dot{y}_2 \\ \dot{y}_3 \end{pmatrix} = \begin{pmatrix} -35 & 35 & 0 \\ -7 & 28 & 0 \\ 0 & 0 & -3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} 0 \\ -y_1 y_3 \\ y_1 y_2 \end{pmatrix} + \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}. \quad (135)$$

Considerando (131), admitindo

$$A = \begin{pmatrix} -35 & 35 & 0 \\ -7 & 28 & 0 \\ 0 & 0 & -3 \end{pmatrix} \quad (136)$$

e resolvendo a equação algébrica não-linear de Riccati através do comando *lqr* do software MATLAB®, obtemos a função de controle

$$u = - \begin{pmatrix} 0,6790 & -5,5836 & 0 \\ -5,5836 & 47,0518 & 0 \\ 0 & 0 & 0,1623 \end{pmatrix} \begin{pmatrix} y_1 - x_1 \\ y_2 - x_2 \\ y_3 - x_3 \end{pmatrix}. \quad (137)$$

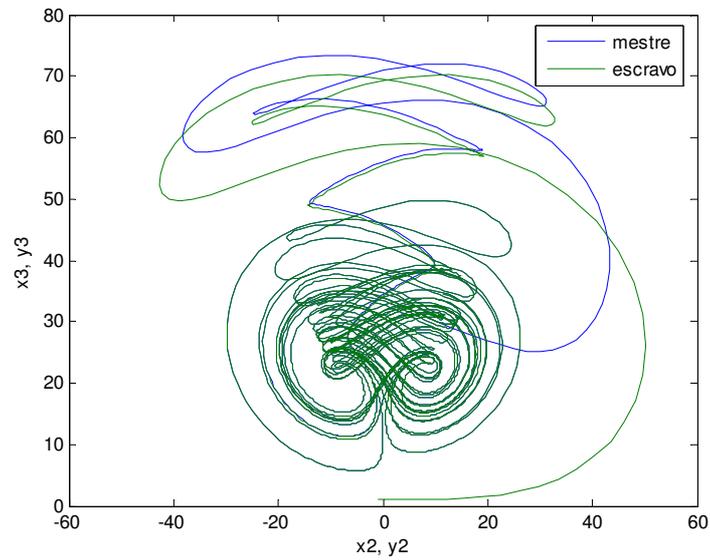


Figura 33 - Dinâmica dos sistemas de Chen em 2D

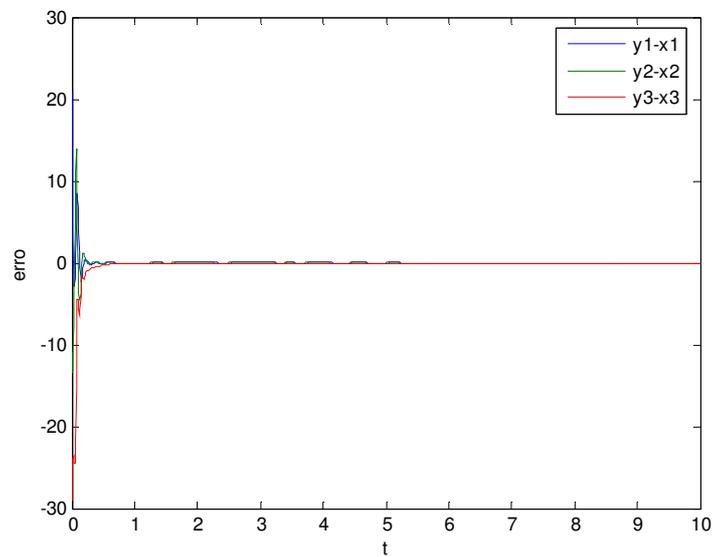


Figura 34 - Erro de sincronização - Sistema de Chen

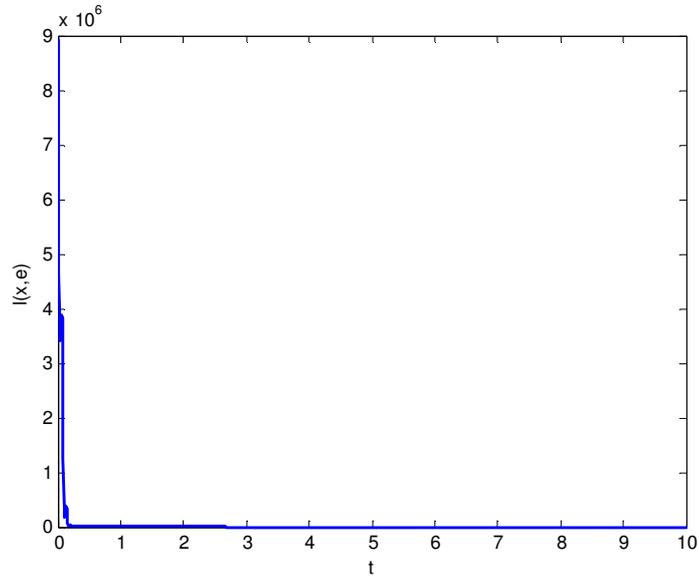


Figura 35 - Avaliação da função $l(x,e)$ - Sistema de Chen

Considerando a teoria da estabilidade de Lyapunov, a avaliação da função $l(x,e)$, definida positiva na trajetória, mostra que o controle aplicado é ótimo e assintoticamente estável.

Sincronização do sistema de Lü. Escrevendo os sistemas mestre (138) e escravo (139) na forma matricial

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{pmatrix} = \begin{pmatrix} -36 & 36 & 0 \\ 0 & 20 & 0 \\ 0 & 0 & -3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{pmatrix}, \quad (138)$$

$$\begin{pmatrix} \dot{y}_1 \\ \dot{y}_2 \\ \dot{y}_3 \end{pmatrix} = \begin{pmatrix} -36 & 36 & 0 \\ 0 & 20 & 0 \\ 0 & 0 & -3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} 0 \\ -y_1 y_3 \\ y_1 y_2 \end{pmatrix} + \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}. \quad (139)$$

Considerando (131), admitindo

$$A = \begin{pmatrix} -36 & 36 & 0 \\ 0 & 20 & 0 \\ 0 & 0 & -3 \end{pmatrix} \quad (140)$$

e resolvendo a equação algébrica não-linear de Ricatti através do comando *lqr* do software MATLAB®, obtemos a função de controle

$$u = - \begin{pmatrix} 0,0139 & 0,0089 & 0 \\ 0,0089 & 40,0410 & 0 \\ 0 & 0 & 0,1623 \end{pmatrix} \begin{pmatrix} y_1 - x_1 \\ y_2 - x_2 \\ y_3 - x_3 \end{pmatrix}. \quad (141)$$

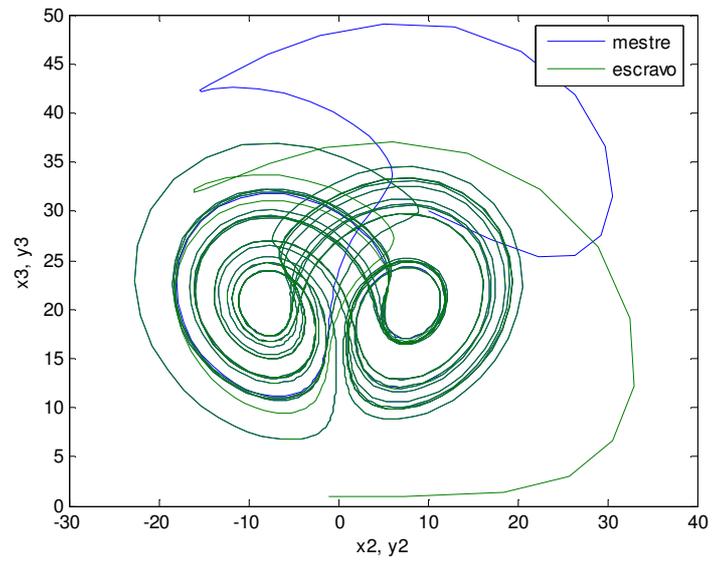


Figura 36 - Dinâmica dos sistemas de Lü em 2D

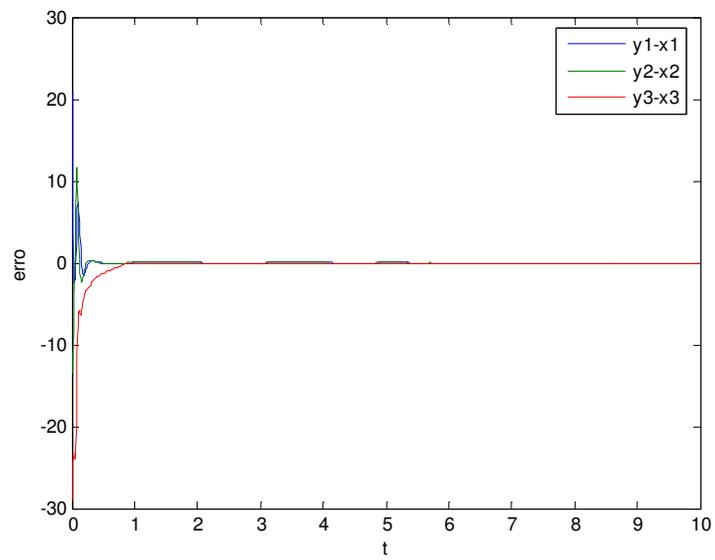


Figura 37 - Erro de sincronização - Sistema de Lü

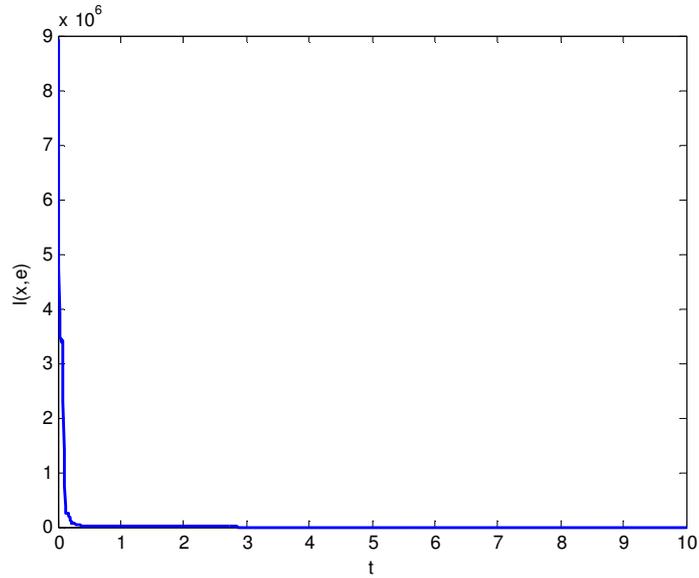


Figura 38 - Avaliação da função $l(x,e)$ – Sistema de Lü

Considerando a teoria da estabilidade de Lyapunov, a avaliação da função $l(x,e)$, definida positiva na trajetória, mostra que o controle aplicado é ótimo e assintoticamente estável.

Sincronização do sistema caótico unificado. A seguir, apresentamos o resultado de duas simulações numéricas da sincronização do sistema para $\alpha = 0,8$, primeiro usando sinal de controle escalar, e a seguir usando sinal de controle vetorial.

Considerando o sistema mestre (38), o sistema escravo toma a forma

$$\begin{aligned} \dot{y}_1 &= (25\alpha + 10)(y_2 - y_1) + u_1 \\ \dot{y}_2 &= (28 - 35\alpha)y_1 - y_1y_3 + (29\alpha - 1)y_2 + u_2 \\ \dot{y}_3 &= y_1y_2 - \left(\frac{\alpha + 8}{3}\right)y_3 + u_3 \end{aligned} \quad (142)$$

onde (u_1, u_2, u_3) são sinais de controle. Representando (142) em forma matricial, obtemos

$$\begin{pmatrix} \dot{y}_1 \\ \dot{y}_2 \\ \dot{y}_3 \end{pmatrix} = \begin{pmatrix} -25\alpha - 10 & 25\alpha + 10 & 0 \\ 28 - 35\alpha & 29\alpha - 1 & 0 \\ 0 & 0 & \frac{(-\alpha - 8)}{3} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} 0 \\ -y_1y_3 \\ y_1y_2 \end{pmatrix} + \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}. \quad (143)$$

Para as simulações a seguir, escolhamos arbitrariamente $\mathbf{x}(\mathbf{0}) = \begin{pmatrix} 1 \\ -1,3 \\ -1 \end{pmatrix}$,

$\mathbf{y}(\mathbf{0}) = \begin{pmatrix} -11 \\ -47 \\ 31 \end{pmatrix}$ e o parâmetro $\alpha = 0,8$.

Sincronização do sistema unificado através de controle escalar. De (143) obtemos

$$A = \begin{pmatrix} -30 & 30 & 0 \\ 0 & 22,2 & 0 \\ 0 & 0 & -2,9333 \end{pmatrix}. \quad (144)$$

Escolhendo

$$Q = \begin{pmatrix} 8000 & 0 & 0 \\ 0 & 8000 & 0 \\ 0 & 0 & 8000 \end{pmatrix}; B = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}; R = 1 \quad (145)$$

e resolvendo a equação algébrica matricial de Riccati através da função *lqr* do software MATLAB®, obtemos o controle linear feedback em forma escalar

$$u_2 = -(27,6640 \quad 122,9605 \quad 0) \begin{pmatrix} y_1 - x_1 \\ y_2 - x_2 \\ y_3 - x_3 \end{pmatrix}. \quad (146)$$

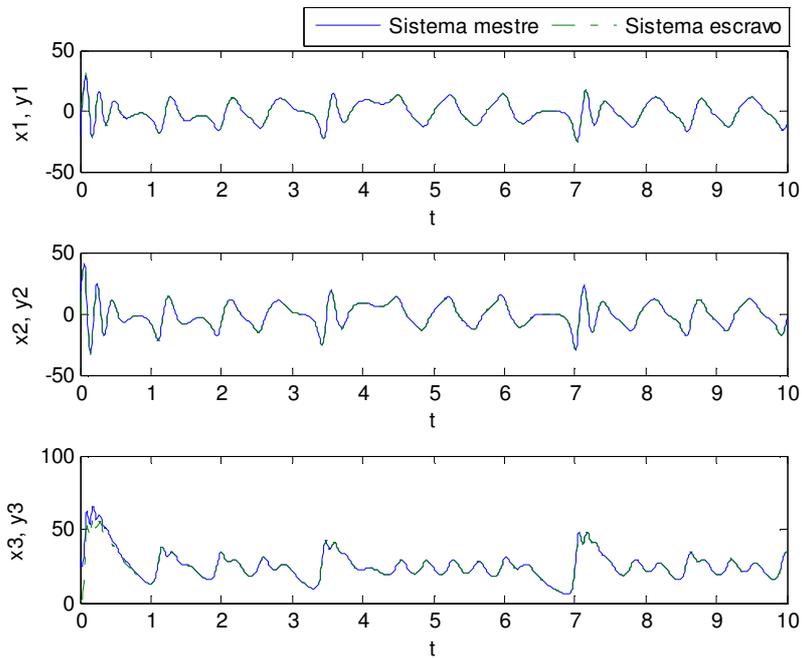


Figura 39 - Sincronização do sistema caótico unificado com controle escalar

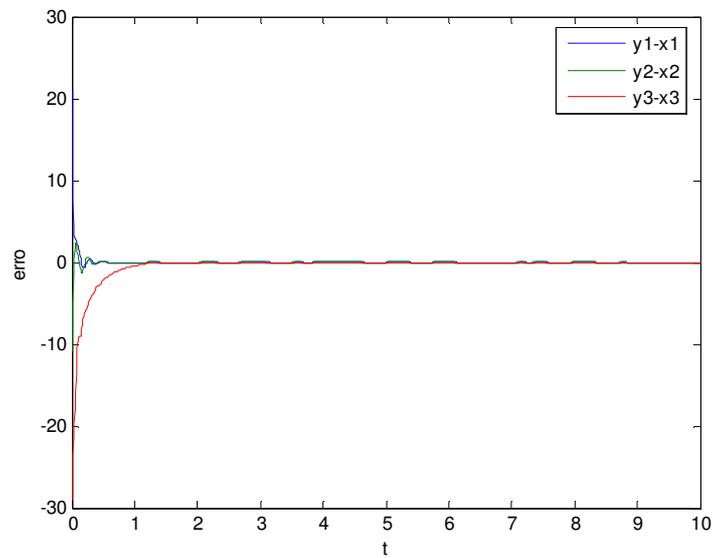


Figura 40 - Erro de sincronização – controle escalar

O erro se aproxima rapidamente de zero, e os sistemas estão assintoticamente sincronizados após aproximadamente 2 segundos.

Sincronização do sistema unificado através de controle vetorial. Considerando-se (144), escolhendo

$$Q = \begin{pmatrix} 8000 & 0 & 0 \\ 0 & 8000 & 0 \\ 0 & 0 & 8000 \end{pmatrix}; B = R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (147)$$

e resolvendo a equação algébrica matricial de Riccati através da função *lqr* do software MATLAB®, obtemos o controle linear feedback em forma vetorial

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = - \begin{pmatrix} 63,7928 & 10,1444 & 0 \\ 10,1444 & 117,0609 & 0 \\ 0 & 0 & 86,5575 \end{pmatrix} \begin{pmatrix} y_1 - x_1 \\ y_2 - x_2 \\ y_3 - x_3 \end{pmatrix}. \quad (148)$$

A Figura 41 mostra o comportamento das variáveis de estado dos sistemas mestre e escravo.

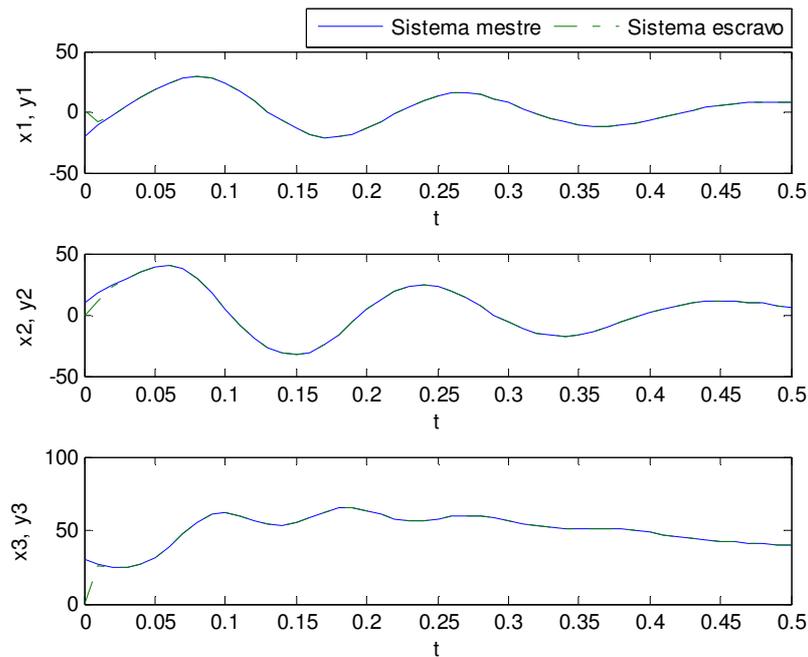


Figura 41 - Sincronização do sistema caótico unificado com controle vetorial

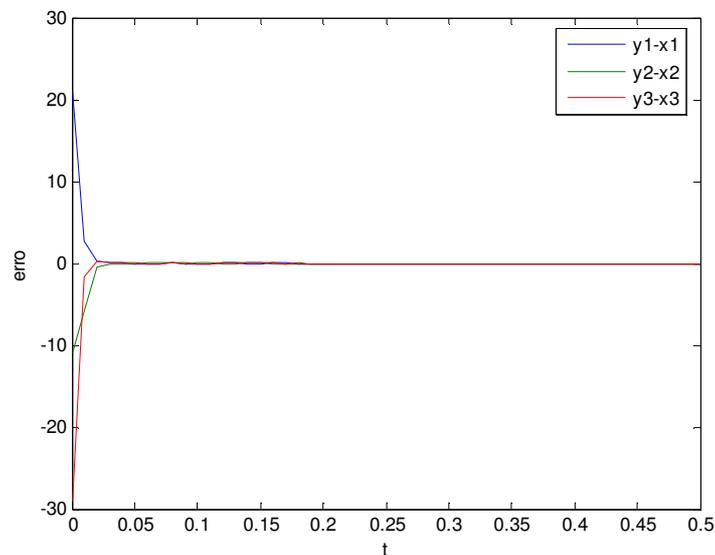


Figura 42 - Erro de sincronização – controle vetorial

O erro se aproxima rapidamente de zero, e os sistemas estão sincronizados após decorrido 0,27 segundo.

4.5 Considerações finais

As simulações mostraram que o controle linear feedback levou os três pares de sistemas *mestre/escravo* à sincronização para as condições testadas. Ao apreciar os enfoques de sincronização de caos considerados no Capítulo 3 e suas características, percebe-se que, sob condições idênticas, o controle ótimo linear feedback apresenta pelo menos três vantagens: quanto ao grau de generalidade, quanto à simplicidade de implementação e quanto ao tempo necessário para levar os sistemas à sincronização.

O grau de generalidade do controle ótimo linear feedback permitiu que todas as simulações realizadas neste capítulo tomassem como base a resolução do problema do controle ótimo feedback formulado e resolvido na seção 4.3. Da mesma forma, para uma grande variedade de sistemas autônomos não-lineares, a metodologia pode ser aplicada diretamente e de forma sistemática.

Devido à forma como o problema do controlador ótimo linear feedback é resolvido, sua solução é relativamente simples se comparada a problemas da programação dinâmica que utilizam a equação de Hamilton-Jacobi-Bellman (125). Isso ocorre porque a

solução do problema do controle ótimo reduz-se a resolução da equação matricial algébrica de Ricatti (121).

Além disso, sob condições idênticas, o desempenho do controle linear feedback mostrou-se superior ao desempenho das demais metodologias estudadas e de diversas metodologias utilizadas em publicações especializadas (como por exemplo em [13, 14, 25, 35, 45, 50]), no que diz respeito ao tempo necessário para a sincronização. Considerando a possibilidade de aumentar a sensibilidade do controle ao erro (116), surge a pergunta: é possível melhorar ainda mais o desempenho do controle no sentido da redução de tempo e custo? A resposta para essa pergunta será investigada no próximo capítulo.

A respeito da otimalidade do controle, a avaliação da função $l(x, e)$, que é definida positiva na trajetória, mostra que o controle aplicado é ótimo e também é estável na trajetória percorrida em todos os casos considerados. Assim, a otimalidade do controle permitiu que recursos fossem poupados, de acordo com um critério desejável durante a tarefa de sincronização.

A forma vetorial e a forma escalar do controle ótimo linear feedback, apresentadas na última subseção deste capítulo, permitem sincronizar o sistema caótico unificado para todo o intervalo do parâmetro $\alpha \in [0, 1]$. Isso significa uma grande evolução em relação à metodologia proposta em [50], que em condições idênticas permite sincronizar os sistemas para $\alpha \in [0, \frac{1}{11}]$.

Conforme esperado, nas simulações realizadas o controle vetorial (u_1, u_2, u_3) levou o sistema em desvios à origem mais rapidamente do que o controle escalar $(0, u_2, 0)$.

5 SELEÇÃO DA MEDIDA DE DESEMPENHO: AVALIAÇÃO DE CUSTO E TEMPO NECESSÁRIO PARA SINCRONIZAÇÃO

5.1 Introdução

De acordo com [39], ao selecionar um funcional J a ser minimizado, também conhecido como índice de desempenho, deve-se definir uma expressão matemática que, quando minimizada, indica que o sistema está desempenhando da maneira mais desejável. Dessa forma, escolher um índice de desempenho significa traduzir o comportamento desejado do sistema em termos matemáticos.

Por exemplo, ponderando as componentes do índice de desempenho de um sistema de controle, é possível fazer com que um automóvel realize determinada trajetória em menor tempo ou, alternativamente, que realize determinada trajetória com menor consumo de combustível, ou ainda que realize determinada trajetória com tempo e consumo de combustível intermediários em qualquer proporção desejada.

Assim, também pode ser desejável que a sincronização ocorra de maneira suficientemente rápida, mesmo que isso implique maior gasto de sinal de controle. Isso significa anuir a um gasto maior de controle em troca da economia de tempo.

Diversos enfoques da sincronização de caos inviabilizam aplicações práticas devido ao excessivo tempo necessário para que osciladores atinjam sincronização. No caso de comunicações, é utópico admitir-se que enfoques que necessitem demasiado tempo para levar os sistemas à sincronia possam ser aplicados na prática, como por exemplo os enfoques sugeridos e utilizados em [13, 14, 25, 35, 45, 50].

No presente capítulo, a metodologia do controle ótimo linear feedback proposta em [64] é avaliada numericamente a fim de considerar o custo do controle, dados pela equação (124), e o tempo gasto até a sincronização. Avaliamos a influência da matriz Q no custo e no tempo necessário para que sistemas mestre e escravo tornem-se síncronos, e procuramos definir os valores de Q que produzem resultados satisfatórios para a aplicação proposta neste trabalho.

Dessa forma, considerando os sistemas caóticos de Lorenz, Chen e Lü e a metodologia de controle linear feedback, o objetivo deste capítulo é responder às seguintes perguntas:

- O aumento dos valores de Q diminui o tempo necessário para sincronização?
- É possível sincronizar em menor tempo e ainda assim reduzir o custo do controle?

5.2 Seleção da medida de desempenho

Seja o índice de desempenho (124). Considerando (128), podemos reescrevê-lo na forma

$$J = \int_0^{\infty} [e^T Q e - h^T(x, e) P e - e^T P h(x, e) + u^T R u] dt \quad (149)$$

onde a matriz Q é a matriz de pesos do erro (atribui um preço a ser pago por erros entre as trajetórias dos sistemas mestre e escravo) e R é a matriz de pesos do sinal de controle (atribui um preço a ser pago pelos valores dos sinais de controle). A natureza quadrática das expressões do custo do erro ($e^T Q e = Q e^2$) e do custo do controle ($u^T R u = R u^2$) indica que maiores valores de e e de u implicam em maior custo final do funcional (149). Como Q e R estão presentes no funcional a ser minimizado, é esperado que o valor final do funcional aumente para valores maiores de Q e R .

Dessa forma, é esperado que para valores maiores de Q o sistema de controle se torne mais sensível a erros e que, como consequência, a sincronização ocorra mais rapidamente. Como os pesos do erro no custo final do índice de desempenho a ser minimizado aumentam, espera-se que a trajetória ótima nesse caso apresente menor erro ainda que maior esforço de controle.

A avaliação do tempo necessário para sincronização consistirá em sincronizar os sistemas diversas vezes, variando o valor dos elementos diagonais da matriz Q , com a finalidade de analisar o custo total do controle, dado pela equação (149) e o tempo necessário para que o sistema em desvios (119) seja conduzido assintoticamente à origem.

Nas simulações, serão consideradas matrizes Q diagonais na forma

$$Q = \begin{pmatrix} q_{11} & 0 & 0 \\ 0 & q_{22} & 0 \\ 0 & 0 & q_{33} \end{pmatrix}, \text{ com } q_{11} = q_{22} = q_{33}. \text{ Como a matriz } Q \text{ entra no funcional (149) na}$$

expressão quadrática $e^T Q e$, de forma que

$$e^T Q e = (e_1 \ e_2 \ e_3) \begin{pmatrix} q_{11} & q_{12} & q_{13} \\ q_{21} & q_{22} & q_{23} \\ q_{31} & q_{32} & q_{33} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} = e_1^2 q_{11} + e_2^2 q_{22} + e_3^2 q_{33} + \dots, \quad (150)$$

verificamos que os termos diagonais multiplicam o quadrado do erro. Daí a importância e influência que os termos diagonais da matriz Q têm no custo total J . Além disso, matrizes diagonais facilitam a sistematização dos resultados e simplificam a investigação numérica.

A avaliação do custo do controle consistirá em simular numericamente a sincronização dos sistemas mestre-escravo para valores crescentes dos elementos da matriz Q , de forma a avaliar o que acontece com o custo e o tempo necessário para sincronização na medida em que os valores aumentam. A resolução da integral (149) equivale ao somatório da norma do sinal de controle (122) durante o tempo de desempenho do sistema, ou seja, o gasto total de sinal de controle na sincronização.

5.3 Simulações numéricas

Simulações numéricas mostram o custo e o tempo gasto na sincronização dos sistemas de Lorenz, Chen e Lü em função dos valores atribuídos a Q , para as condições

$$\text{iniciais } x_0 = \begin{pmatrix} -20 \\ 10 \\ 30 \end{pmatrix} \text{ e } y_0 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}. \text{ O tempo está expresso em segundos, e o custo do}$$

controle está expresso em unidades e diz respeito ao somatório das normas do sinal de controle aplicado em todos os passos de integração, até que seja atingida a condição $\|e\| = 0$. O custo também pode ser entendido como o resultado da integral (149), calculada na trajetória percorrida.

Sistema de Lorenz. A Figura 43, a Figura 44 e a Figura 45 apresentam os

gráficos do tempo e custo da sincronização para o sistema de Lorenz em função dos valores de Q .

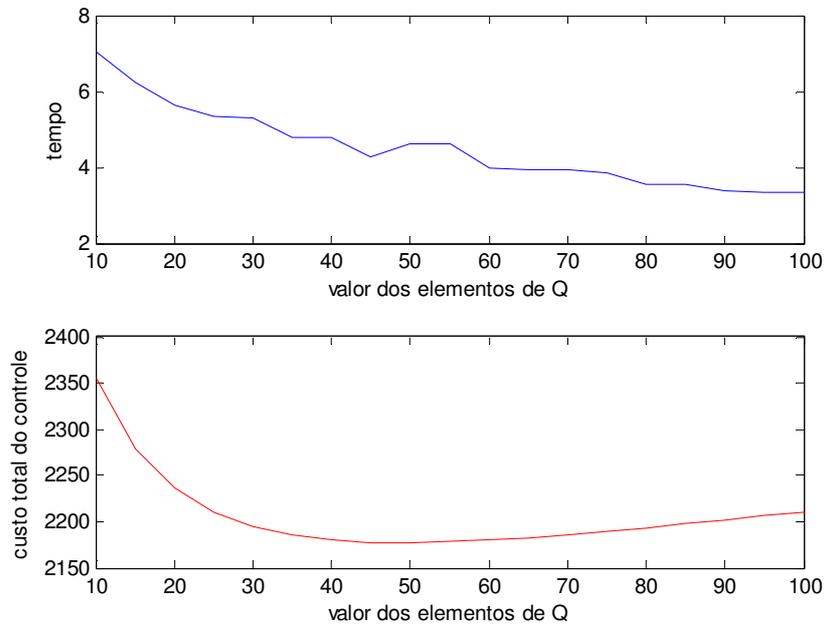


Figura 43 - Tempo e custo da sincronização - sistema de Lorenz, $q_{ii}=10$ a $q_{ii}=100$

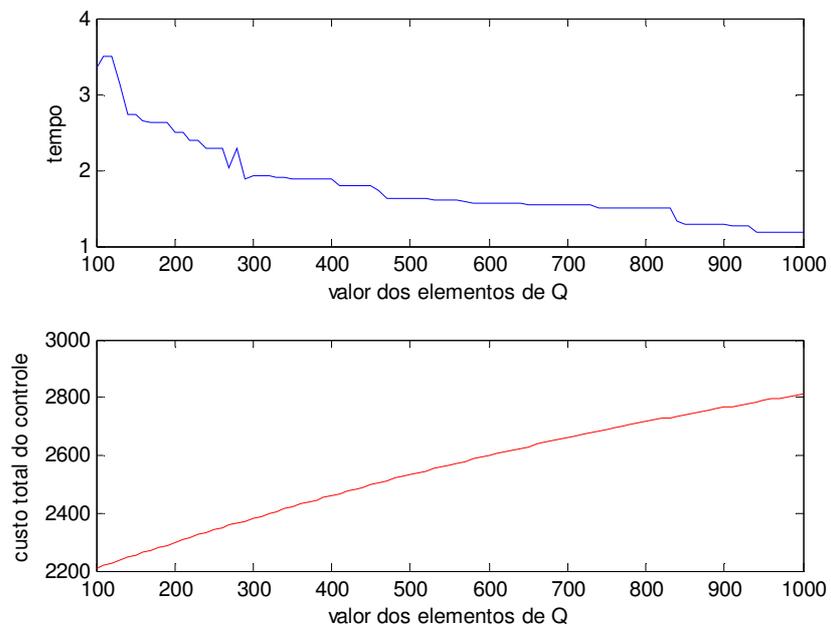


Figura 44 - Tempo e custo da sincronização - sistema de Lorenz, $q_{ii}=100$ a $q_{ii}=1000$

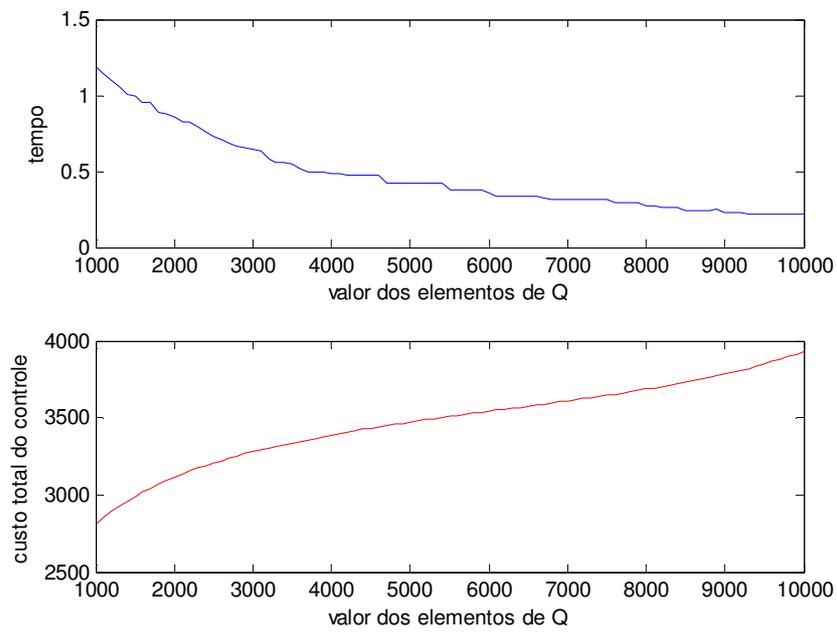


Figura 45 - Tempo e custo da sincronização - sistema de Lorenz, $q_{ii}=1000$ a $q_{ii}=10000$

Sistema de Chen. A Figura 46, a Figura 47 e a Figura 48 apresentam os gráficos do tempo e custo da sincronização para o sistema de Lü em função dos valores de Q .

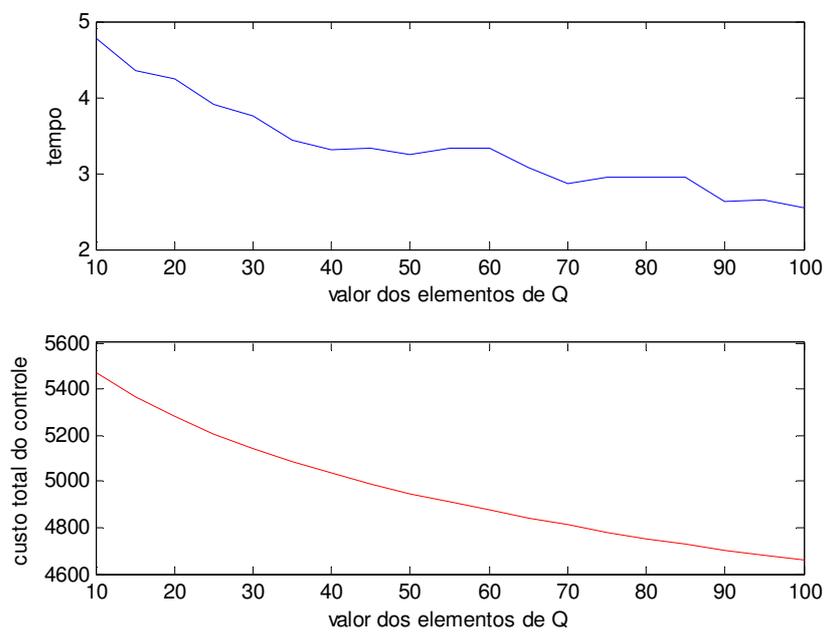


Figura 46 - Tempo e custo da sincronização - sistema de Chen, $q_{ii}=10$ a $q_{ii}=100$

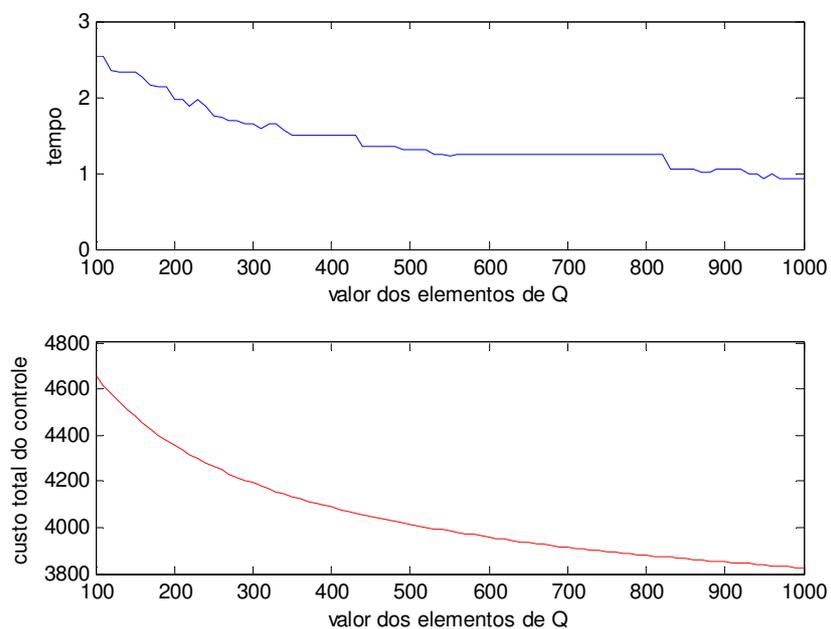


Figura 47 - Tempo e custo da sincronização - sistema de Chen, $q_{ii}=100$ a $q_{ii}=1000$

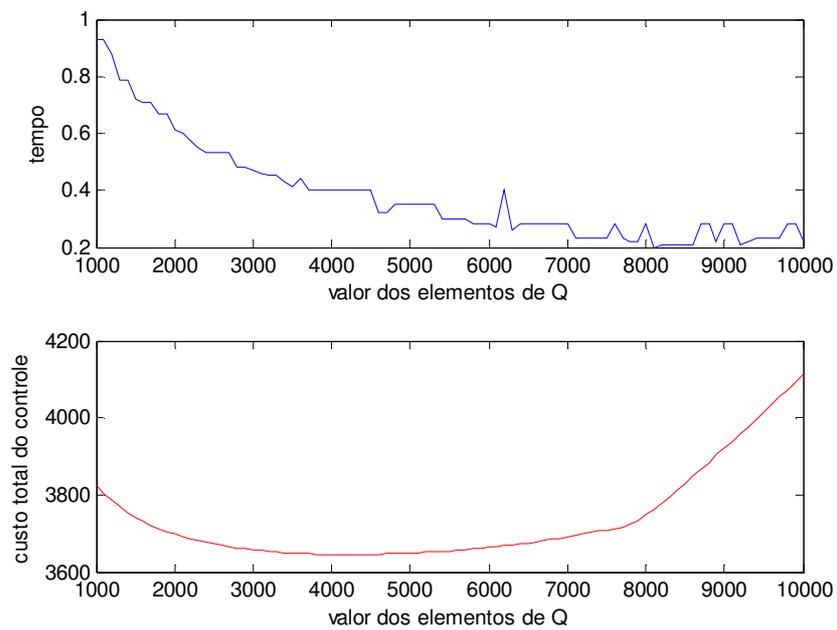


Figura 48 - Tempo e custo da sincronização - sistema de Chen, $q_{ii}=1000$ a $q_{ii}=10000$

Sistema de Lü. A Figura 49, a Figura 50 e a Figura 51 apresentam os gráficos do tempo e custo da sincronização para o sistema de Lü em função dos valores de Q .

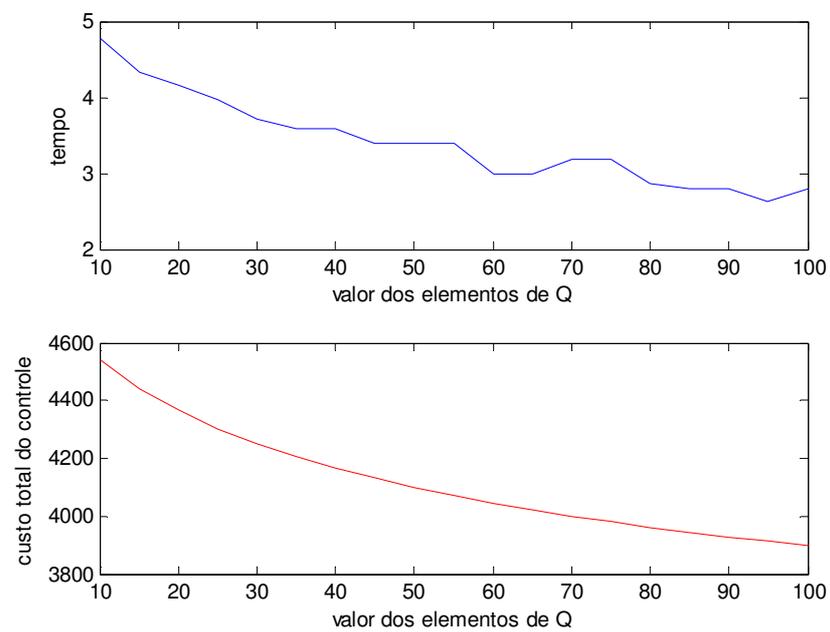


Figura 49 - Tempo e custo da sincronização - sistema de Lü, $q_{ii}=10$ a $q_{ii}=100$

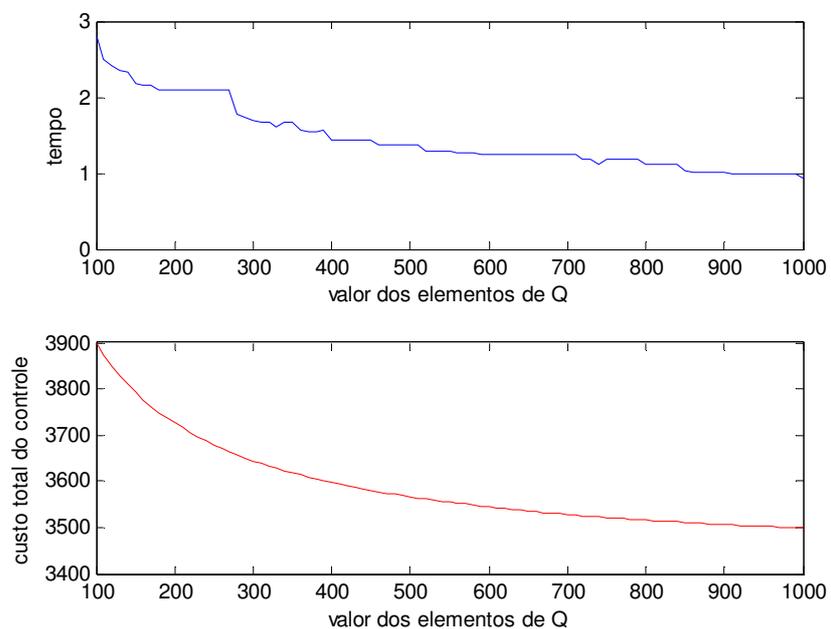


Figura 50 - Tempo e custo da sincronização - sistema de Lü, $q_{ii}=100$ a $q_{ii}=1000$

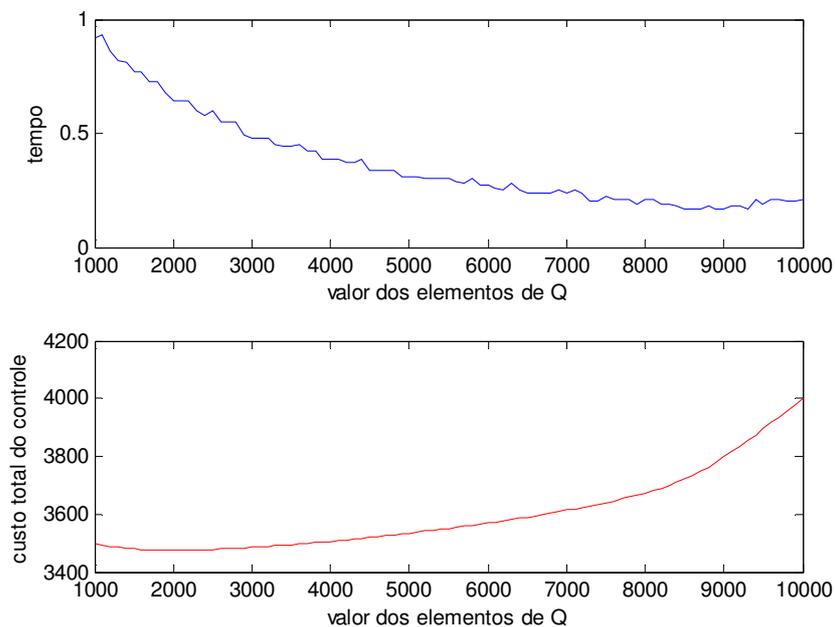


Figura 51 - Tempo e custo da sincronização - sistema de Lü, $q_{ii}=1000$ a $q_{ii}=10000$

Sistematização dos resultados. O desempenho do controle ótimo linear feedback é apresentado abaixo. A primeira coluna de dados serve como referência para as demais, que são apresentadas em termos percentuais.

Sistema de Lorenz

	$q_{ii} = 10$	$q_{ii} = 10^2$	$q_{ii} = 10^3$	$q_{ii} = 10^4$
Tempo (s)	8,00	-56,25%	-85,00%	-97,14%
Custo (J)	2350	-5,95%	+19%	+65,95%

Sistema de Chen

	$q_{ii} = 10$	$q_{ii} = 10^2$	$q_{ii} = 10^3$	$q_{ii} = 10^4$
Tempo (s)	5,00	-50,00%	-80,00%	-95,60%
Custo (J)	5500	-14,90%	-36,36%	-25,45%

Sistema de Lü

	$q_{ii} = 10$	$q_{ii} = 10^2$	$q_{ii} = 10^3$	$q_{ii} = 10^4$
Tempo (s)	4,80	-41,67%	-79,17%	-95,41%
Custo (J)	4570	-14,67%	-23,41%	-12,47%

5.4 Considerações finais

É visto que maiores valores dos elementos da matriz Q , de uma forma geral, diminuem o tempo necessário para que a sincronização ocorra. Como mencionado anteriormente, Q é a matriz de pesos do erro, e por esse motivo, maiores valores de Q significam maior sensibilidade do controle a erros.

Assim, considerando uma matriz diagonal Q formada por elementos $q_{11} = q_{22} = \dots = q_{mm}$, conclui-se que, em geral, é possível sincronizar os sistemas mestre/escravo mais rapidamente aumentando-se os valores de seus elementos. A título de exemplo, o tempo necessário para sincronizar o sistema de Chen diminuiu 92% quando o valor dos elementos diagonais de Q foram aumentados de 10 para $4 \cdot 10^3$. Além disso, para o mesmo caso, o custo total do controle diminuiu 27%.

A respeito do custo total do controle, as simulações mostram que determinado intervalo de valores de Q pode, ao mesmo tempo, diminuir o tempo de sincronização e o custo total do controle.

Consideramos a seguir as perguntas cujas respostas foram investigadas neste capítulo. Considerando o formato da matriz Q utilizada nas simulações e considerando os resultados obtidos, é possível observar que:

- de uma forma geral, o aumento dos elementos da matriz Q diminui o tempo necessário para que o controle linear feedback estabilize o sistema em desvios na origem;
- o aumento dos valores de Q pode, ao mesmo tempo, diminuir o tempo e o custo total do controle.

A menor tolerância a erros implica menor tempo de atuação do controle e, nas simulações realizadas, menor tempo de atuação do controle significou redução no custo J .

Em situações extremas consideradas, com $Q = 10^4 \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, o controle ótimo linear

feedback levou os sistemas mestre/escravo à sincronia em $t = 0,2$ segundo para os sistemas de Chen e Lü, e em $t = 0,25$ segundo para o sistema de Lorenz.

Comparativamente, a metodologia que obteve melhor desempenho dentre as apresentadas no capítulo 3 necessitou cerca de 3 segundos para levar os sistemas mestre/escravo à sincronia aproximada, com $\|e\| \cong 0$ e aproximadamente 6 segundos para levá-los à sincronia absoluta, ou seja, para $\|e\| = 0$.

6 SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS VIA CONTROLE LINEAR FEEDBACK CONTÍNUO POR PARTES

6.1 Introdução

Em aplicações práticas de sistemas de controle, nem sempre é possível que o controle atue durante todo o tempo em que o sistema está desempenhando, devido a limitações físicas, técnicas, econômicas e etc. Como limitações dessas naturezas estão presentes em grande parte dos sistemas reais, é importante estudar a maneira como os métodos de controle se comportam e até que ponto eles podem dar uma boa resposta nesse caso. Exemplos de aplicações em que descontinuidades no sinal de controle estão presentes são o controle de pragas e o funcionamento de um condicionador de ar.

Da mesma forma, como controle implica custo nas mais diversas formas, pode ser desejável que um sistema seja mantido sob controle sem que ele seja controlado efetivamente o tempo inteiro.

O objetivo deste capítulo é testar a metodologia do controle linear feedback segundo a metodologia proposta em [64] para a sincronização de sistemas caóticos sob essa perspectiva de descontinuidades no sinal de controle, ou seja, de controle contínuo por partes.

6.2 O controle linear feedback contínuo por partes

Considerando a metodologia do controle ótimo linear feedback apresentada no capítulo 4 e definindo

$$\mathbf{u} \triangleq \begin{cases} \mathbf{u}, & t \in [nT - \varepsilon, nT + \varepsilon], \\ 0, & \text{caso contrário.} \end{cases} \quad (151)$$

onde T é um período arbitrário de tempo, $n \in N$ é o n -ésimo período e $0 < \varepsilon \leq \frac{T}{2}$ é uma constante positiva, obtém-se a metodologia do controle linear feedback em forma contínua por partes.

A cada período T haverá um intervalo de tempo $[nT - \varepsilon, nT + \varepsilon]$ em que u estará efetivamente controlando o sistema, que desempenhará livre no tempo restante. Para $\varepsilon = \frac{T}{2}$, o controle linear feedback contínuo por partes equivale à sua forma contínua, conforme apresentada no capítulo 4.

Cabe ressaltar que o intervalo de tempo em que u estará efetivamente controlando o sistema está relacionado com restrições econômicas, físicas e técnicas e, dessa forma, será definido arbitrariamente nas simulações para fins de teste. Assim, o tempo de atuação do controle é escolhido arbitrariamente, não obedece a critérios de otimização e também não é resultado de um processo de otimização. Por outro lado, a trajetória descrita pelo sistema, enquanto controlado, é ótima no sentido de que o sistema em desvios é conduzido à origem de forma que a trajetória minimize o índice de desempenho J .

Dessa forma, o controle u para $t \in [nT - \varepsilon, nT + \varepsilon]$ é ótimo no sentido de conduzir a trajetória do sistema escravo à trajetória do sistema mestre minimizando o funcional J dado por (124) durante o seu tempo de atuação.

A condição que garante a estabilidade do controle linear feedback para sistemas não-lineares, definida como a positividade definida da função (120) para o caso do controle contínuo, pode ser estendida para o caso do controle contínuo por partes. Uma vez que a avaliação é realizada na trajetória ótima, se a função $l(x, e)$ for definida positiva, então o controle u é estável e transfere o sistema em desvios (119) de qualquer condição inicial à condição final $\lim_{t \rightarrow \infty} e(t) = 0$ de maneira ótima.

No intervalo para o qual $u = 0$, o sistema em desvios retomará as perturbações e as trajetórias deverão divergir até que o controle seja acionado novamente. Essas perturbações cessam naturalmente quando a condição final $\lim_{t \rightarrow \infty} e(t) = 0$ é satisfeita, caso no qual os sistemas mestre e escravo estão assintoticamente sincronizados.

6.3 Simulações Numéricas

Esta seção apresenta simulações da aplicação do controle linear feedback contínuo por partes, conforme proposto em [33], para o sistema de Lorenz. As simulações

foram realizadas para $T=1$, $x_0 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$, $y_0 = \begin{pmatrix} -2 \\ 1 \\ 3 \end{pmatrix}$. Para o sistema de Lorenz original,

tomamos a matriz dos termos lineares

$$A = \begin{pmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -8/3 \end{pmatrix}, \text{ escolhendo } B = R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, Q = \begin{pmatrix} 2000 & 0 & 0 \\ 0 & 2000 & 0 \\ 0 & 0 & 2000 \end{pmatrix} \text{ e}$$

resolvendo a equação algébrica de Riccati através do comando *lqr* do software

MATLAB®, obtemos $P = \begin{pmatrix} 42,5691 & 17,0232 & 0 \\ 17,0232 & 44,2954 & 0 \\ 0 & 0 & 42,1341 \end{pmatrix}$ e, como consequência, o

controlador ótimo linear feedback, $u = - \begin{pmatrix} 42,5691 & 17,0232 & 0 \\ 17,0232 & 44,2954 & 0 \\ 0 & 0 & 42,1341 \end{pmatrix} \begin{pmatrix} y_1 - x_1 \\ y_2 - x_2 \\ y_3 - x_3 \end{pmatrix}$.

Seguem abaixo as simulações para os valores $\varepsilon = 0,02$ e $\varepsilon = 0,01$ que representam atividade da função de controle durante aproximadamente 5% e 3% do tempo total de desempenho, respectivamente.

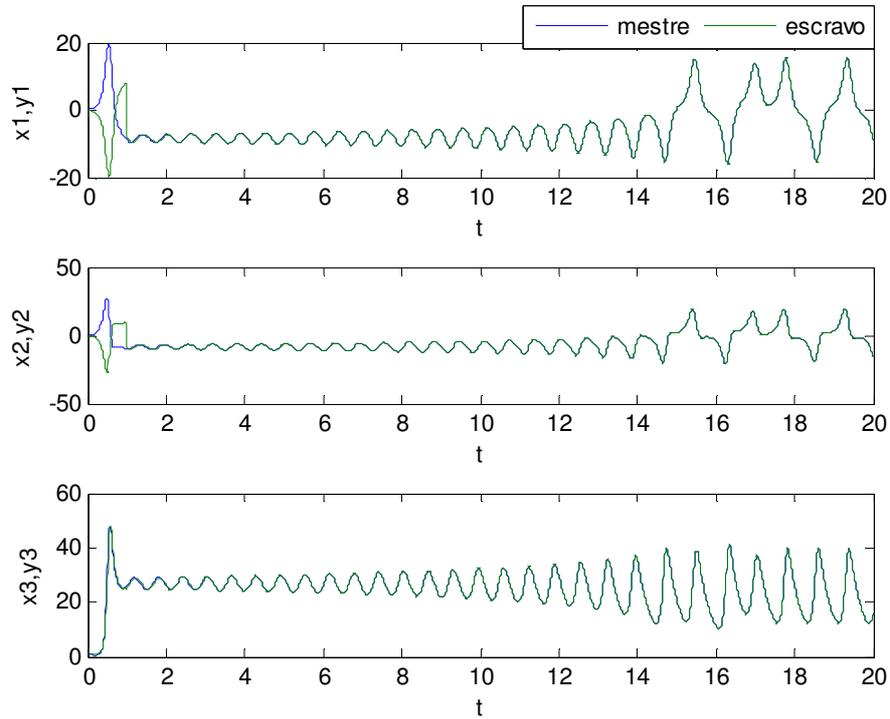


Figura 52 - Sincronização do sistema de Lorenz via controle contínuo por partes, $\epsilon=0.02$

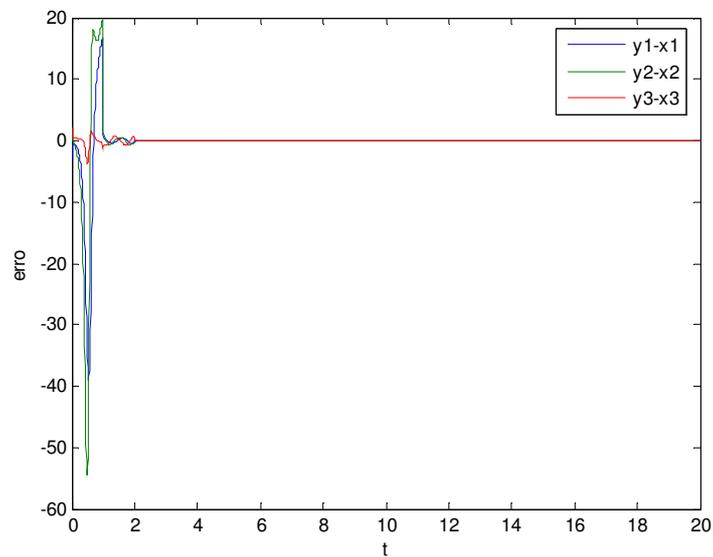


Figura 53 – Erro de sincronização do sistema de Lorenz via controle contínuo por partes, $\epsilon=0,02$

A Figura 52 e a Figura 53 mostram que o controle linear feedback contínuo por partes leva os sistemas de Lorenz à sincronização após aproximadamente 3 segundos,

mesmo com o tempo de atuação do controlador reduzido para 5% do tempo efetivo de desempenho dos sistemas.

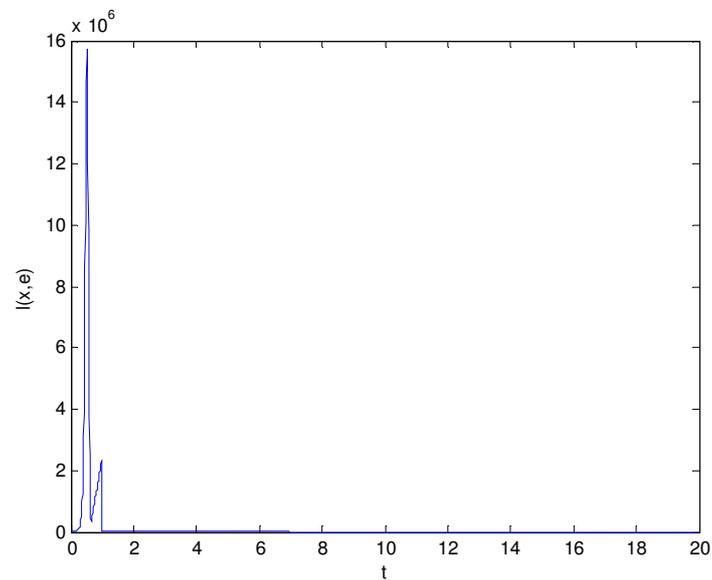


Figura 54 - Avaliação da função $l(x,e)$ na trajetória, $\varepsilon=0,02$

A Figura 54 mostra que é satisfeita a condição suficiente para a estabilidade e otimalidade do controle linear feedback, ou seja, a função $l(x,e) \geq 0$ na trajetória. A Figura 55 e a Figura 56 apresentam o resultado da sincronização para $\varepsilon = 0,01$, que ocorre após aproximadamente 6 segundos.

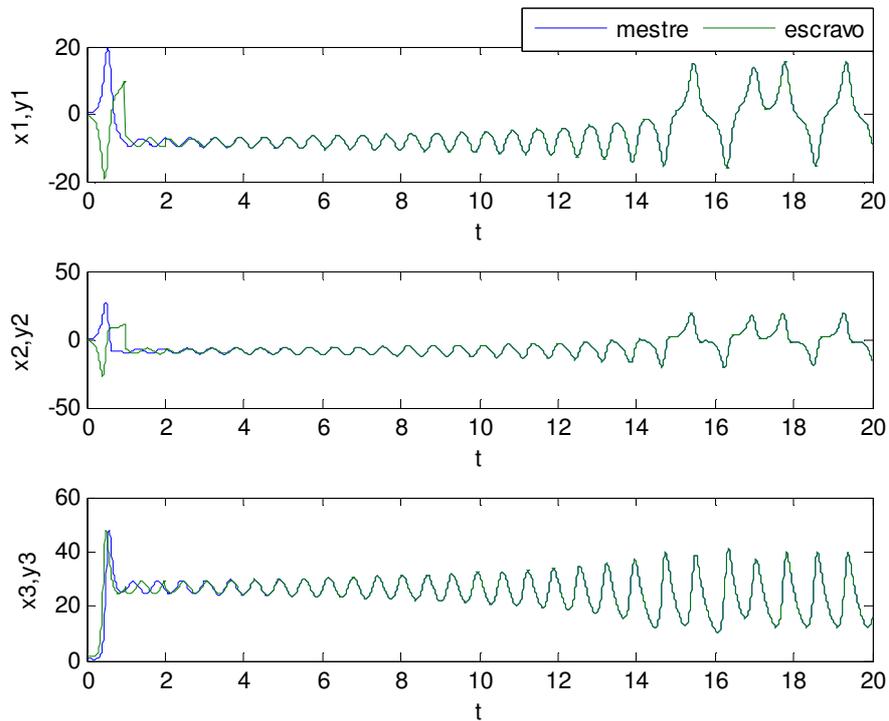


Figura 55 – Sincronização sistema de Lorenz via controle contínuo por partes, $\varepsilon=0,01$

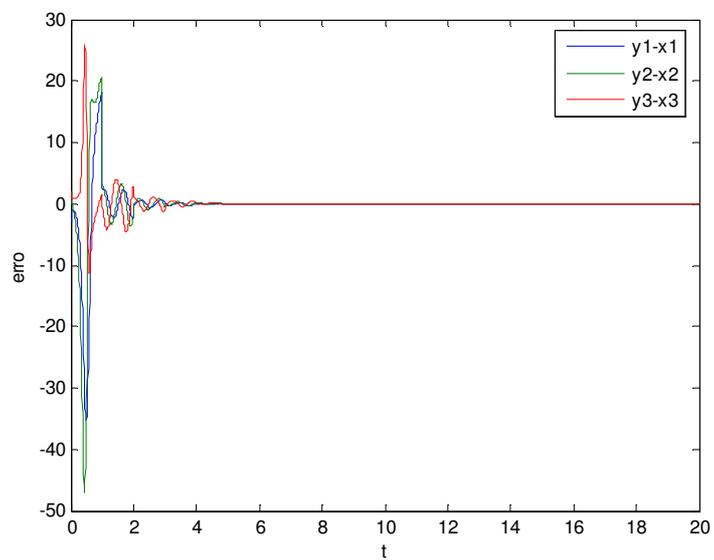


Figura 56 - Erro de sincronização sistema de Lorenz via controle contínuo por partes, $\varepsilon=0,01$

A Figura 57 mostra que a função $l(x, e) \geq 0$ na trajetória. e, portanto, o controle é ótimo e estável na trajetória.

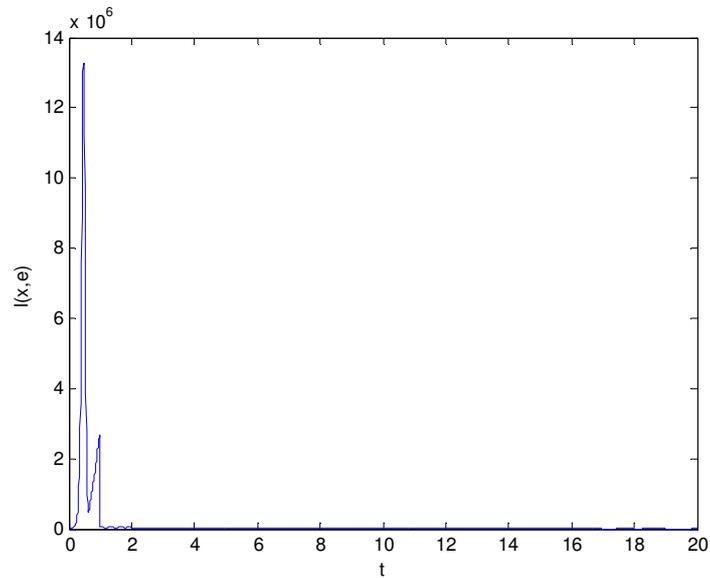


Figura 57 - Avaliação da função $l(x,e)$ na trajetória, $\varepsilon=0,01$

6.4 Considerações finais

Verificamos que, para o sistema de Lorenz, o controle linear feedback contínuo por partes é efetivo ao levar os sistemas mestre/escravo à sincronização, mesmo quando drasticamente reduzido seu tempo de atuação, conforme mostra a Figura 58.

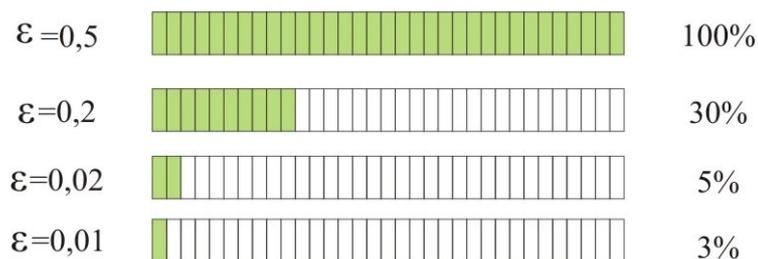


Figura 58 - Tempo aproximado de atuação do controle em relação ao tempo total de desempenho do sistema

É interessante mencionar que a matriz $Q = \begin{pmatrix} 2000 & 0 & 0 \\ 0 & 2000 & 0 \\ 0 & 0 & 2000 \end{pmatrix}$ foi utilizada

nas simulações e que a função de controle obtida a partir da resolução da equação matricial algébrica de Ricatti (121) controlou satisfatoriamente o sistema em desvios resultante e o

conduziu assintoticamente à zero. Entretanto, para simulações realizadas com valores

menores da diagonal principal, como por exemplo $Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, a função de controle

resultante conduz o sistema em desvios à aproximadamente zero, ou seja, decorrido um tempo arbitrário t , $\|e\| \cong 0$. Assim, o sistema em desvios retoma as perturbações tão logo $u = 0$ e, apesar de controlado, o erro não vai assintoticamente a zero.

Assim, através dos exemplos apresentados, foi possível deixar claro que existe a possibilidade do uso do controle linear feedback em situações em que a aplicação de controle contínuo não é desejável ou não é possível. Nesses casos, considerando os resultados obtidos neste capítulo, fica claro que o controle linear feedback contínuo por partes constitui-se em uma alternativa.

O resultado positivo obtido no presente capítulo aumenta em importância ao considerarmos que grande parte dos sistemas reais não podem ser controlados ininterruptamente. Assim, ao transportar o conceito de continuidade por partes para a metodologia do controle linear feedback, novas possibilidades foram abertas no sentido de que aumenta a gama de sistemas para os quais o controle linear feedback pode ser testado e aplicado.

7 SINCRONIZAÇÃO DE CAOS APLICADA À COMUNICAÇÃO SEGURA

7.1 Introdução

De acordo com [71], todas as formas de comunicação sem fio são baseadas em sincronização. Por exemplo, sintonizar um rádio em determinada estação “trava” o receptor na frequência de transmissão. Quando a sincronização ocorre, a música é extraída por um processo chamado demodulação, que separa a música do sinal que a carrega.

A partir da descoberta de que osciladores caóticos podem ser controlados e sincronizados, tão logo surgiu a idéia de utilizá-los em sistemas de comunicação [60], com o objetivo de utilizar a dinâmica complexa de um sistema caótico para transportar mensagens. A vantagem é que além de transportar a mensagem, o sinal caótico pode mascarar a mensagem transmitida.

A próxima seção deste capítulo é dedicada a alguns elementos da criptografia clássica por dois motivos: o primeiro deles é que muitas publicações que tratam da comunicação segura utilizando sinais caóticos utilizam a nomenclatura estabelecida da criptografia clássica; o segundo é que grande parte dos princípios da criptografia clássica podem ser estendidos aos sistemas criptográficos baseados em caos.

A terceira seção, de forma geral e simplificada, apresenta três tipos de esquemas de comunicação segura baseados em sincronização através de sinais analógicos, a máscara caótica aditiva, a modulação caótica e o criptossistema caótico.

A quarta seção apresenta um esquema criptográfico baseado em caos, do qual alguns elementos são utilizados no sistema proposto no capítulo oito.

Tendo em vista explorar elementos da aplicação de sistemas caóticos em comunicação, o presente capítulo tem por objetivos:

- introduzir elementos históricos e a nomenclatura estabelecida da comunicação segura;

- encadear os elementos da comunicação e criptografia clássica nos conceitos de sincronização e caos;
- apresentar exemplos de aplicações propostas na literatura.

7.2 Princípios básicos da comunicação segura

A comunicação em geral está intimamente relacionada com a idéia de sigilo. É o caso de transações bancárias, estratégias de guerra e de marketing, segredos corporativos, governamentais, industriais e de privacidade pessoal, para citar alguns.

Sigilo na comunicação é obtido através da criptografia, que é a arte e ciência da escrita cifrada, de manter informações em segredo. A criptanálise é o estudo das maneiras de subverter o processo utilizado para criptografar. A combinação da criptografia e da criptanálise dá origem ao termo criptologia [15, 21, 28, 67].

A informação que se deseja manter em segredo é chamada texto simples ou texto claro; criptógrafos desenvolvem algoritmos de criptografia; criptanalistas estudam os algoritmos em busca de fraquezas, e os invasores procuram subverter os algoritmos para ter acesso a informações [15, 51, 74].

Depois de sofrer o processo de encriptação um texto claro se torna um texto encriptado, que se torna novamente um texto claro ao sofrer o processo inverso, a decriptação.

Os algoritmos de encriptação e decriptação funcionam a partir de uma chave. A chave é um conjunto de letras e números que determina de que forma o texto claro será encriptado pelo algoritmo. Uma chave é chamada simétrica quando a mesma seqüência de letras e números é utilizada tanto para encriptar quanto para decriptar os dados. Do contrário, é chamada assimétrica.

Na criptografia clássica, conforme [5], uma chave k é geralmente uma seqüência de bits gerada automaticamente, de tal forma que se uma chave é constituída por n bits, então qualquer possível chave de n bits deve ter igual probabilidade 2^{-n} . O conjunto de todas as r chaves possíveis é chamado de espaço da chave $K = \{k_1, k_2, \dots, k_r\}$.

De acordo com [15], existem vários motivos pelos quais a chave é necessária. O

mais relevante é que invasores sempre descobrem o algoritmo, seja por dedução, roubo, chantagem, extorsão, engenharia reversa ou análise criptográfica. A história da criptografia não possui registro de um único algoritmo que tenha sido mantido em segredo. Outro motivo é que, quando publicados, os algoritmos podem ser analisados e eventuais fraquezas detectadas.

Algoritmos públicos são os algoritmos cujas instruções são públicas e notórias de quem possa interessar-se; algoritmos secretos são algoritmos cujas instruções são mantidas em segredo por um grupo seletivo de usuários.

Podemos definir matematicamente as relações entre texto-claro, texto-cifrado, espaço da chave e suas relações da seguinte maneira [5]:

- P é um conjunto finito de possíveis textos-claros;
- C é um conjunto finito de possíveis textos-cifrados;
- K é um conjunto finito de possíveis chaves;
- E é um conjunto finito de todas as regras de encriptação;
- D é um conjunto finito de todas as regras de decifração;
- Para cada $k \in K$, existe uma regra de encriptação $e_k \in E$ e uma regra correspondente de decifração $d_k \in D$. Cada $e_k : P \rightarrow C$ e $d_k : C \rightarrow P$ são funções tais que $d_k(e_k(p)) = p$ para cada texto-claro $p \in P$.

De acordo com [21], a segurança de algoritmos secretos depende do nível de segredo com que a estrutura do algoritmo pode ser guardada. Por esse motivo, esse tipo de algoritmo só pode ser usado para comunicação privada com pequeno número de participantes e, em geral, algoritmos públicos são escolhidos na maior parte das aplicações.

Ainda de acordo com [21], para criptanálise de algoritmos públicos, assume-se que:

- o invasor conhece a estrutura do algoritmo e a probabilidade da chave k que é utilizada;
- o invasor tem acesso ao canal público, de modo que obtém um segmento arbitrário do texto cifrado.

De acordo com [15, 38], todo e qualquer algoritmo de criptografia pode ser

quebrado¹⁵, e os melhores algoritmos são simplesmente os que podem suportar um ataque por mais tempo. Assim, um algoritmo é suficientemente seguro quando ataques bem-sucedidos se concretizam quando a informação já não tem mais relevância para o invasor.

De acordo com [28], a criptografia tem papel fundamental na comunicação e computação, pois:

- pode proteger informações armazenadas em computadores ou em trânsito de um computador para outro contra acessos não-autorizados;
- pode ser usada para detectar alterações intencionais ou acidentais em dados;
- pode ser usada para verificar se o autor de um documento é mesmo quem você pensa que é;

Ainda de acordo com [28], apesar das vantagens, a criptografia tem limitações:

- não pode evitar que um invasor apague dados;
- um invasor pode descobrir uma maneira de decifrar mensagens cifradas com o algoritmo que você está usando;
- um invasor pode acessar arquivos antes de serem encriptados ou depois de decriptados.

Diferentes algoritmos possuem diferentes resistências a ataques, e essa resistência deve-se a uma combinação de fatores:

- o nível de segredo com que a chave pode ser guardada;
- a dificuldade de adivinhar a chave ou tentar todas as chaves possíveis;
- a dificuldade de inverter o algoritmo de encriptação sem conhecer a chave de encriptação;
- a existência ou falta de falhas ou maneiras adicionais de decifrar o arquivo.

Tendo em vista os aspectos práticos do uso da criptografia, existem algumas características que todo sistema criptográfico deve possuir [5]:

- fácil implementação;
- custo aceitável;

¹⁵ Diz-se de um algoritmo que é subvertido.

- segurança dependente apenas de sua chave;
- conhecimento parcial da chave nunca deve revelar informação parcial do texto claro nem da parte desconhecida da chave;
- dois textos cifrados encriptados com chaves ligeiramente diferentes devem ser completamente diferentes;
- para duas chaves ou dois textos claros com uma pequena diferença, nenhuma diferença distinguível deve ser encontrada nos respectivos textos cifrados pelos métodos conhecidos de análise estatística.
- o texto cifrado deve ser estatisticamente indistinguível da saída de uma função verdadeiramente aleatória.
- O sistema deve ser testado quanto à vulnerabilidade aos ataques específicos a sistemas caóticos.
- O sistema deve ser suficientemente seguro contra ataques de força bruta;

Os principais tipos de ataque existentes contra algoritmos de encriptação são [44, 78]:

- somente texto-cifrado (*cyphertext only*): o invasor tem acesso a frações arbitrariamente grandes de um ou mais textos cifrados.

- texto claro conhecido (*known-plaintext*): o invasor tem acesso a parte do texto claro e do correspondente texto cifrado.

- texto claro escolhido (*chosen-plaintext*): o invasor tem acesso ao algoritmo de encriptação, e logo pode escolher alguns textos claros e obter os respectivos textos cifrados.

- texto-cifrado escolhido (*chosen-cyphertext*): o invasor tem acesso ao algoritmo de decifração e pode escolher alguns textos cifrados e obter os respectivos textos claros.

Um ataque de força bruta é aquele em que todas as combinações possíveis são utilizadas, até que a verdadeira chave é encontrada. Em média, é necessária uma busca em 50% do espaço de chaves nesse tipo de ataque. Um bit a mais na chave representa a duplicação do espaço de chaves, de forma que dobra o tempo necessário para um ataque.

7.3 Comunicação segura baseada em caos

Esta seção apresenta algumas idéias e conceitos que ligam a criptografia baseada em caos à criptografia clássica e apresenta as idéias que baseiam três esquemas de comunicação baseados em caos.

Idéias e conceitos básicos. Podemos traçar paralelos entre características de sistemas caóticos e de sistemas criptográficos clássicos, de acordo com a tabela abaixo, extraída de [5] e traduzida pelo autor:

Propriedade caótica	Propriedade criptográfica	Descrição
Ergodicidade	Confusão	A saída tem a mesma distribuição para qualquer entrada
Sensibilidade às condições iniciais	Difusão com uma pequena mudança no <i>texto claro</i> ou na <i>chave</i>	Uma pequena diferença na entrada pode causar uma grande mudança na saída
Mistura	Difusão com uma pequena mudança em um bloco do <i>texto claro</i>	Uma pequena diferença na área local pode causar uma grande diferença no espaço como um todo
Dinâmica determinística	Pseudo-aleatoriedade determinística	Um processo determinístico pode causar um comportamento pseudo-aleatório
Complexidade da estrutura	Complexidade do algoritmo	Um processo simples pode apresentar alto grau de complexidade.

Tabela 1 – Paralelos entre propriedades da criptografia baseada em caos e clássica

Máscara caótica aditiva [20, 57]. O esquema foi concebido em 1993 por Cuomo e Oppenheim foi chamado de *additive chaotic masking*. O esquema consiste em sistemas mestre/escravo idênticos, onde uma das variáveis de estado do sistema mestre é utilizada como máscara onde o sinal da mensagem é adicionado, originando o sinal que será transmitido. O sinal da mensagem deve ser tipicamente de 20 a 30dB mais fraco do que o sinal da máscara caótica para que a sincronização ocorra [78].

Como a máscara caótica possui dinâmica complexa e o sinal da mensagem adicionada é consideravelmente menor do que a máscara, de forma a ficar camuflado, de imediato pode parecer impossível extrair a mensagem sem conhecer exatamente a máscara que a camufla. Entretanto, o esquema da máscara caótica aditiva possui um nível de

segurança baixo e já foi quebrado de diversas maneiras [3], mesmo sem conhecimento algum dos sistemas usados para mascarar a mensagem.

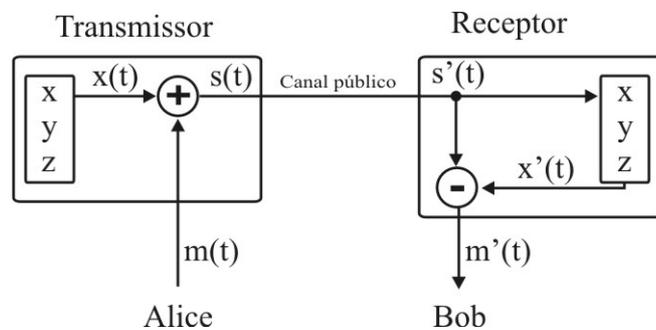


Figura 59 - Máscara caótica aditiva

Modulação caótica. A segunda geração de sistemas de comunicação segura baseados na sincronização de sistemas caóticos foi desenvolvida entre 1993 e 1995, ficou conhecida como modulação caótica e subdivide-se em modulação de parâmetros e modulação não-autônoma.

Na modulação de parâmetros o sinal da mensagem é utilizado para mudar os parâmetros do sistema transmissor/mestre, de forma que suas trajetórias desenvolvem-se em torno de diferentes atratores, de acordo com o sinal da mensagem $m(t)$. No sistema receptor/escravo, um controle adaptativo é utilizado para sintonizar adaptativamente seus parâmetros, levando o erro entre transmissor e receptor para aproximadamente zero. Dessa forma, é possível para o receptor extrair a mensagem $m(t)$. Como o sistema transmissor muda constantemente de atrator, a dinâmica de suas variáveis de estado é muito mais complexa do que a de um sistema caótico em um único atrator.

A modulação caótica não-autônoma utiliza o sinal da mensagem para alterar o espaço de fases do sistema transmissor/mestre. Assim, o sistema transmissor oscila entre diferentes órbitas do mesmo atrator através de uma perturbação dependente do sinal da mensagem $m(t)$.

A segunda geração aumentou consideravelmente o nível de segurança dos algoritmos ao aumentar a complexidade do comportamento do sistema transmissor. Apesar disso, a exemplo dos esquemas da primeira geração, já foram subvertidos e não oferecem um nível satisfatório de segurança [4, 5].

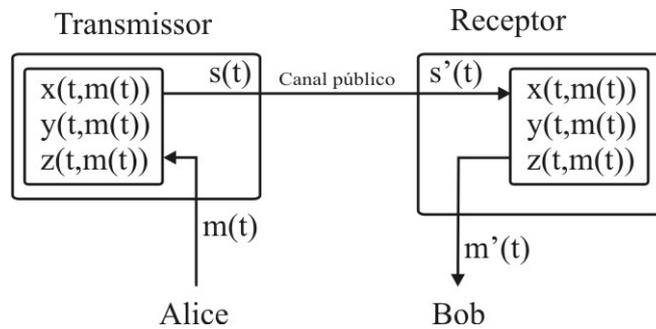


Figura 60 - Modulação caótica

Criptossistema caótico. A terceira geração é conhecida como criptossistema caótico e foi concebida no final da década de 90 com o intuito de aumentar a segurança oferecida pelos esquemas das gerações anteriores, combinando técnicas da criptografia clássica e da sincronização caótica.

Nesse esquema, a mensagem $m(t)$ é encriptada por uma regra dependente de uma chave $k(t)$, que por sua vez é gerada pelo sistema transmissor/mestre. O sinal é então utilizado para dirigir o sistema caótico, de forma que sua dinâmica é alterada continuamente de uma maneira muito complexa [78]. Então, outra variável de estado do sistema é transmitida através de um canal público, que pode ser acessado pelo intruso. Desde que o intruso não tenha acesso à chave $k(t)$, é muito difícil recuperar a mensagem $m(t)$ a partir do sinal transmitido. Ainda de acordo com [78], esse tipo de encriptação ainda não foi subvertida.

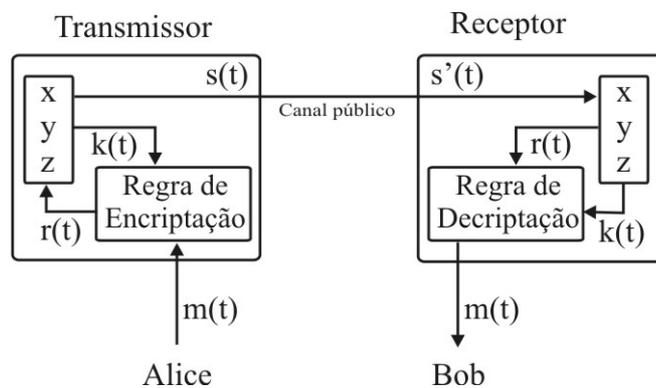


Figura 61 - Criptossistema caótico

Ataques criptográficos específicos a esquemas caóticos. De acordo com [5], além dos ataques conhecidos pela criptografia clássica, existem três possibilidades de ataque a um sistema criptográfico baseado em caos:

- Extrair a mensagem $m(t)$ diretamente do sinal transmitido $c(t)$;
- Extrair o sinal caótico $x(t)$ do sinal transmitido $c(t)$ para recuperar a mensagem $m(t)$;
- Estimar os parâmetros do sistema utilizado para gerar o sinal caótico a partir do sinal transmitido $c(t)$;

7.4 Estudo de um algoritmo de encriptação baseado em caos

No capítulo 4, utilizamos o controle linear feedback para sincronizar o sistema unificado para o intervalo $[0,1]$ de um parâmetro α . Nesta seção utilizamos esse resultado para admitir o sistema caótico unificado, conforme apresentado no capítulo 2, como base de um sistema criptográfico. O resultado da sincronização obtido no capítulo 4 permite utilizar esse intervalo $\alpha \in [0,1]$ como espaço da chave do sistema criptográfico. Dessa forma, pretende-se tornar o algoritmo mais seguro contra ataques de força-bruta se comparado ao esquema apresentado em [50], no qual o espaço da chave fica restrito ao intervalo $[0, \frac{3}{116}]$, [33, 50]. Apresentamos a seguir um algoritmo proposto em [68] e adaptado em [34] para utilização em sistemas de comunicação baseados em sincronização.

O processo consiste em duas etapas distintas: a sincronização dos osciladores e a transferência do sinal caótico que carrega a mensagem. Omitimos as simulações da sincronização do sistema caótico unificado, cujos resultados podem ser visitados no capítulo 4.

As equações do sistema transmissor (152) e receptor (153) são mostradas a seguir:

$$\begin{cases} \dot{x}_1 = (25\alpha + 10)(x_2 - x_1) \\ \dot{x}_2 = (28 - 35\alpha)x_1 - x_1x_3 + (29\alpha - 1)x_2 + Am, \\ \dot{x}_3 = x_1x_2 - \frac{1}{3}(\alpha + 8)x_3 \end{cases} \quad (152)$$

$$\begin{cases} \dot{y}_1 = (25\alpha + 10)(y_2 - y_1) \\ \dot{y}_2 = \dot{x}_2 + u_2 \\ \dot{y}_3 = y_1 y_2 - \left(\frac{\alpha + 8}{3}\right) y_3 \\ m = \frac{1}{A}(\dot{x}_2 - (28 - 35\alpha)y_1 + y_1 y_3 - (29\alpha - 1)y_2) \end{cases}, \quad (153)$$

onde m é a mensagem, A é uma constante que tem o objetivo de diminuir a amplitude da mensagem em relação ao sinal caótico, α é um parâmetro, e u_2 é o sinal de controle.

Na primeira etapa, os sistemas transmissor e receptor são sincronizados na forma mestre/escravo. O sistema receptor é controlado e sua trajetória é levada à do sistema transmissor, de forma que o erro entre as trajetórias seja levado ao zero, ou seja, $\|e\| = 0$, e então $u_2 = 0$.

Na segunda etapa, inicia-se em (152) o processo de encriptação e transmissão do sinal \dot{x}_2 , que é recebido e decriptado na quarta equação de (153), de acordo com a idéia proposta em [68].

No contexto da criptografia, o parâmetro α trabalha como a chave do sistema criptográfico, e assim $k \in [0, 1]$.

As simulações apresentadas contemplam a encriptação de uma imagem I e um parágrafo de texto T . Para a encriptação da imagem, as linhas da matriz de intensidade de brilho dos *pixels* que compõe a imagem são concatenadas e a matriz é transformada em um vetor; cada *pixel* é representado por um número inteiro que pertence ao intervalo $[0, 255]$. No caso do texto, os caracteres são convertidos em código ASCII, e passam a ser um número inteiro no intervalo $[0, 127]$. Cada elemento do vetor m é adicionado à segunda equação do sistema transmissor em um passo de integração [50, 76].

$$I = \begin{pmatrix} i_{11} & i_{12} & \cdots & i_{1n} \\ i_{21} & i_{22} & \cdots & i_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ i_{m1} & i_{m2} & \cdots & i_{mn} \end{pmatrix} \rightarrow (i_{11} \ i_{12} \ \cdots \ i_{1n} \ i_{21} \ \cdots \ i_{2n} \ \cdots \ i_{m1} \ \cdots \ i_{mn})$$

$$T = abcdefgh \rightarrow 97 \ 98 \ 99 \ 100 \ 101 \ 102 \ 103 \ 104$$

Nas simulações, os sistemas são integrados através do método de Runge-Kutta de 4ª ordem, com passo de integração $h = 0,01$ e $A = 10^{-6}$. Apresentamos o resultado da aplicação do algoritmo à notória “foto de Lenna¹⁶” e a um parágrafo de texto. A Figura 62, a Figura 63 e a Figura 64 mostram a imagem original, a encriptada e a recuperada pelo sistema receptor.



Figura 62 - Imagem original

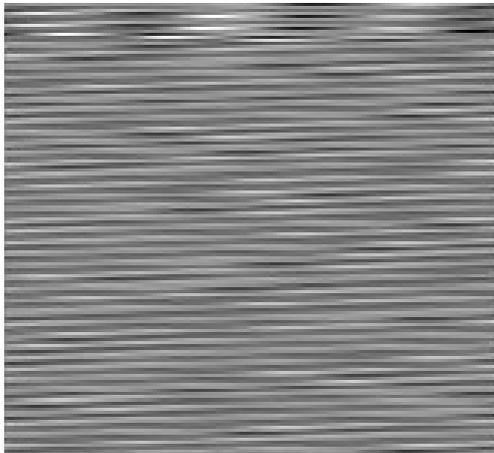


Figura 63 - Imagem encriptada

¹⁶ “Lenna picture” é um padrão para trabalhos em processamento de imagens.

Quando o espaço da chave é definido para sistemas criptográficos baseados em caos, é necessário que os intervalos de valores que os parâmetros podem assumir sejam cuidadosamente testados para que sejam evitados conjuntos de parâmetros que produzam dinâmica não-caótica. Conforme verificado no capítulo 2, o sistema caótico unificado apresenta dinâmica caótica para todo o intervalo $\alpha \in [0,1]$ e possui riqueza de atratores dentro desse intervalo. Assim, três atratores topologicamente não-equivalentes existem dentro do intervalo $\alpha \in [0,1]$ e cada um deles pode ser orbitado, de acordo com o valor do parâmetro α . Por isso, apesar de equações de apresentação simples, o sistema caótico unificado possui dinâmica complexa e versatilidade para a aplicação em comunicação segura.

O esquema apresentado em [34] e reproduzido neste capítulo não é suficientemente seguro, assim como outros esquemas que utilizam parâmetros constantes; ele pode ser quebrado sistematicamente através da utilização de métodos de otimização, conforme verificado em [69].

Assim, o próximo capítulo torna a considerar o algoritmo apresentado em [34], efetuando modificações que consideram a forma de ataque proposta em [69], com o objetivo de corrigir as fraquezas existentes.

8 PROPOSTA DE UM ALGORITMO DE ENCRIPÇÃO BASEADO EM SINCRONIZAÇÃO DE CAOS

8.1 Introdução

Os capítulos anteriores dedicaram-se ao estudo de elementos que formam a base matemática e criptográfica necessárias para a aplicação proposta neste capítulo. No capítulo anterior, apresentamos o algoritmo de encriptação baseado no que foi proposto em [68] e que foi adaptado em [34] para aplicação em sistemas de comunicação baseados em sincronização de caos.

Neste capítulo será apresentada uma alteração no algoritmo para aumentar seu nível de segurança, através da adoção de um mapa caótico unidimensional que regerá o comportamento do parâmetro α do sistema caótico unificado. Tal medida tem por objetivo tornar o parâmetro α não-constante e assim satisfazer uma condição necessária para que o algoritmo torne-se invulnerável ao ataque proposto em [69].

Os resultados de simulações numéricas do funcionamento do algoritmo serão considerados para os casos de canal ideal (sem presença de ruído). O nível de sensibilidade da chave será testado através de simulações de tentativa de decifração utilizando chaves incorretas. Tal informação é fundamental para verificar se chaves minimamente diferentes produzem tentativas frustradas de recuperação da mensagem durante o processo de decifração. Essa é uma característica desejável de um sistema criptográfico, conforme já mencionado no capítulo anterior.

Por fim, o capítulo discute aspectos do algoritmo relacionados à segurança, custo computacional e desempenho na presença de ruído.

Os objetivos do presente capítulo são:

- apresentar o algoritmo proposto em [34] e propor uma modificação para aumentar seu nível de segurança;
- simular numericamente a encriptação e decifração de imagens através do algoritmo;

- analisar o desempenho do algoritmo.

8.2 Algoritmo de encriptação baseado em sincronização de caos

Esta seção apresenta o algoritmo que será proposto e discutido neste capítulo. O funcionamento do algoritmo consiste em duas etapas distintas: a sincronização dos osciladores e a transferência do sinal caótico que carrega a mensagem.

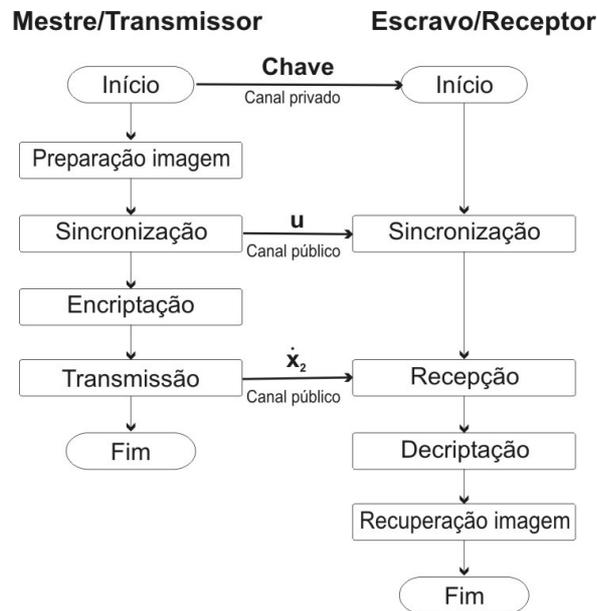


Figura 65 - Esquema de funcionamento do algoritmo

As equações do sistema transmissor (154) e receptor (155), cuja forma baseia-se em [68], são apresentadas a seguir:

$$\begin{cases} \dot{x}_1 = (25\alpha + 10)(x_2 - x_1) \\ \dot{x}_2 = (28 - 35\alpha)x_1 - x_1x_3 + (29\alpha - 1)x_2 + Am, \\ \dot{x}_3 = x_1x_2 - \frac{1}{3}(\alpha + 8)x_3 \end{cases} \quad (154)$$

$$\begin{cases} \dot{y}_1 = (25\alpha + 10)(y_2 - y_1) \\ \dot{y}_2 = \dot{x}_2 + u_2 \\ \dot{y}_3 = y_1y_2 - (\alpha + 8)y_3 \end{cases}, \quad (155)$$

$$m = \frac{1}{A}(\dot{x}_2 + (28 - 35\alpha)y_1 - y_1y_3 + (29\alpha - 1)y_2)$$

onde m é a mensagem, A é uma constante que tem o objetivo de diminuir a amplitude da mensagem em relação ao sinal caótico, α é um parâmetro, e u_2 é o sinal de controle.

Para aumentar o nível de segurança e ampliar o espaço da chave e, considerando a sugestão oferecida em [69] acerca do uso de funções não-lineares limitadas para reger o comportamento dos parâmetros do sistema criptográfico, propomos a utilização de um mapa caótico linear por partes (*piecewise linear chaotic map*) para reger o comportamento do parâmetro α dos sistemas transmissor/receptor. Assim, o parâmetro α dos sistemas (154) e (155) para o passo de integração n será dado por:

$$\alpha_n = \begin{cases} \frac{\alpha_{n-1}}{p}, & \text{se } 0 \leq \alpha_{n-1} < p \\ \frac{(1-\alpha_{n-1})}{(1-p)}, & \text{se } p \leq \alpha_{n-1} < 1 \end{cases} \quad (156)$$

onde $k = (\alpha_0, p)$, com $\alpha_0 \in [0,1]$, $p \in [0,1]$, e $\alpha_0 \neq p$, é a chave do sistema criptográfico.

Considerando a precisão de 16 casas decimais, então temos aproximadamente 10^{16} possibilidades de escolha de α_0 . Para respeitar a condição $\alpha_0 \neq p$, temos $9 \cdot 10^{15}$ possibilidades de escolha de p , e assim a dimensão do espaço da chave K é dado por:

$$\dim\{K\} = 9 \cdot 10^{15} \cdot 10^{16} = 9 \cdot 10^{31} \quad (157)$$

Na primeira etapa, os sistemas transmissor e receptor são sincronizados na forma mestre/escravo, e a trajetória do sistema receptor é levada à do sistema transmissor, de forma que o erro entre as trajetórias seja levado ao zero, ou seja, $\|e\| = 0$, e então $u_2 = 0$. Na segunda etapa, inicia-se o processo de encriptação e transmissão do sinal \dot{x}_2 , que é recebido e decriptado na quarta equação do sistema (155).

As simulações apresentadas contemplam a encriptação de uma imagem (“Lenna picture”). Para a encriptação da imagem, as linhas da matriz de intensidade de brilho dos *pixels* que compõe a imagem são concatenadas e a matriz é transformada em um vetor; cada *pixel* é representado por um número inteiro que pertence ao intervalo $[0, 255]$. Cada elemento do vetor m é adicionado à segunda equação do sistema transmissor em um passo de integração.

8.3 Simulações numéricas

Alguns resultados da aplicação do algoritmo são mostrados abaixo. A integração dos sistemas foi realizada através do método de Runge-Kutta de quarta ordem, com passo de integração $h=0,005$ e $A=10^{-6}$.

Como já foi mostrado numericamente no capítulo 4, o sistema caótico unificado pode ser sincronizado através do uso do controle ótimo linear feedback. Assim, omitiremos os resultados e gráficos da sincronização dos osciladores neste capítulo.

Desempenho do algoritmo. Simulamos a seguir o funcionamento do algoritmo.



Figura 66 – Lenna Picture original (tons de cinza)

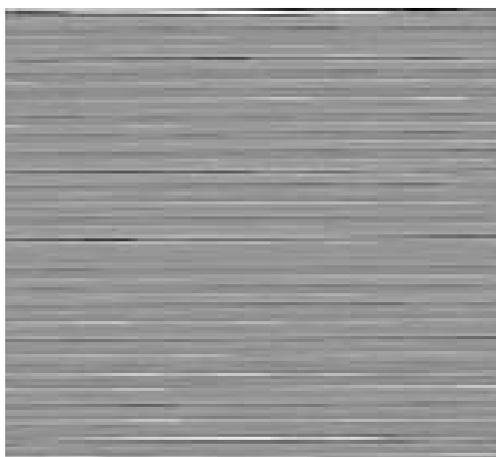


Figura 67 – Lenna picture encriptada (tons de cinza)



Figura 68 - Lenna Picture recuperada (tons de cinza)

A imagem recuperada I_r é exatamente igual à imagem original I_o , ou seja, considerando I_r e I_o como matrizes com dimensão $m \times n$, então $I_o - I_r = 0$. No caso da imagem colorida, de dimensão $m \times n \times a$, onde $a = 3$ para o sistema de cores RGB, temos, para cada uma das cores (vermelho (r), verde (g) e azul (b)), $I_o^r - I_r^r = I_o^g - I_r^g = I_o^b - I_r^b = 0$.



Figura 69 - Lenna Picture original (padrão RGB)



Figura 70 - Lenna Picture encriptada (padrão RGB)



Figura 71 - Lenna Picture recuperada (padrão RGB)

Para ilustrar o teste da sensibilidade do algoritmo à chave, apresentamos a seguir resultados da deciptação da imagem utilizando uma chave incorreta. Para encriptação, utilizamos a chave $k_e = \begin{pmatrix} \alpha_0 \\ p \end{pmatrix} = \begin{pmatrix} 0,5 \\ 0,3 \end{pmatrix}$ e para deciptação

$$k_{d_1} = \begin{pmatrix} \alpha_0 \\ p \end{pmatrix} = \begin{pmatrix} 0,5 \\ 0,3 \end{pmatrix} + \begin{pmatrix} 10^{-16} \\ 0 \end{pmatrix} \text{ e } k_{d_2} = \begin{pmatrix} \alpha_0 \\ p \end{pmatrix} = \begin{pmatrix} 0,5 \\ 0,3 \end{pmatrix} + \begin{pmatrix} 0 \\ 10^{-16} \end{pmatrix}.$$

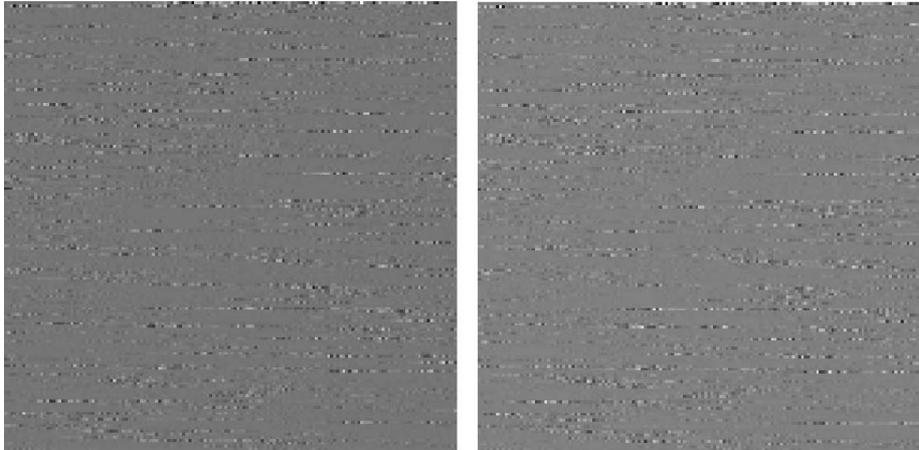


Figura 72 - Tentativa de deciptação utilizando chave incorreta

Conforme mostrado na Figura 72, a imagem não foi recuperada com sucesso pela chave incorreta, a despeito de as diferenças $k_e - k_{d_1} = \begin{pmatrix} 10^{-16} \\ 0 \end{pmatrix}$ e $k_e - k_{d_2} = \begin{pmatrix} 0 \\ 10^{-16} \end{pmatrix}$ serem extremamente pequenas. Isso significa que o algoritmo é extremamente sensível à chave.

8.4 Considerações finais

Esta seção aborda aspectos importantes que dizem respeito ao algoritmo proposto neste capítulo.

Segurança. De acordo com [69], os métodos conhecidos e já utilizados para criptanálise de algoritmos de encriptação caóticos com parâmetros constantes não são eficazes para o caso de parâmetros variáveis e dependentes de funções não-lineares. Mesmo que as funções sejam conhecidas por eventuais subversores, a tarefa de recuperar a chave correta a partir de um segmento arbitrariamente grande do sinal caótico transmitido é uma tarefa para a qual não existem métodos sistemáticos conhecidos.

A respeito de ataques de força bruta, [5] aponta que um algoritmo suficientemente forte possui espaço da chave $K > 2^{100}$. Considerando as chaves $\alpha_0 \in [0,1]$ e $p \in [0,1]$ com precisão de 10^{16} , de tal forma que $\alpha_0 \neq p$, obtemos um espaço de chave $K \approx 10^{31}$ e, nesse caso, $K > 2^{100}$.

Considerando as simulações realizadas para o caso de condições ideais, erros de 10^{-16} na chave são o suficiente para que a mensagem recuperada seja absolutamente ininteligível, o que significa que o algoritmo é extremamente sensível à chave. Por um lado, o valor exato da chave recupera perfeitamente a imagem transmitida; por outro, um erro da ordem de 10^{-16} torna a imagem recuperada tão confusa e ininteligível quanto a imagem encriptada.

Custo de processamento. A idéia central da comunicação baseada em sinais caóticos é obter confusão e difusão de uma maneira reversível, substituindo as operações algébricas da criptografia clássica pela dinâmica determinística, complexa e pseudo-aleatória de osciladores caóticos. Como os osciladores caóticos são passíveis de implementação em hardware, é possível obter considerável redução no custo do processamento de tais operações. Além disso, em aplicações como a comunicação via rádio, o processo todo pode ser conduzido através de equipamentos simples e sem maior sofisticação, como foi mostrado por Cuomo e Oppenheim em [20].

Apresentamos abaixo os dados referentes ao desempenho do algoritmo proposto neste capítulo. As simulações numéricas foram realizadas numa CPU de 1,6GHz. Os tempos de encriptação e decriptação são dados em milissegundos, o tamanho em *bytes* e a taxa em *bytes* por segundo.

Tipo	Encriptação (ms)	Decriptação(ms)	Tamanho (<i>bytes</i>)	Taxa (<i>bytes/s</i>)
Imagem	156	78	961	6k
Texto	62	63	825	13k

Outras considerações. Evidências numéricas mostram que a o mapa caótico unidimensional utilizado para reger o comportamento do parâmetro α é extremamente sensível a erro no valor da chave, o que é um ponto positivo e fundamental.

CONCLUSÕES

No presente trabalho, a dinâmica rica e complexa de alguns sistemas caóticos foi explorada para estudar métodos de sincronização propostos na literatura e para a aplicação de tais sistemas em comunicação segura. Os resultados obtidos foram importantes em dois sentidos: em primeiro lugar, pelo progresso obtido no estudo da aplicação do controle ótimo linear feedback para sincronização de sistemas não-lineares; em segundo lugar, pelo projeto e publicação de um algoritmo de criptografia baseado em sincronização de caos.

O progresso na pesquisa da metodologia do controle ótimo linear feedback para sistemas não-lineares foi obtido em duas direções:

- no estudo do tempo e do sinal de controle gastos na sincronização e sua relação com a matriz de pesos do erro Q ;
- a incorporação do conceito de continuidade por partes na metodologia do controle ótimo linear feedback, que permite a ampliação da gama de sistemas para os quais o controle ótimo linear feedback pode ser aplicado em situações reais.

Os resultados obtidos e relatados no capítulo 5 acrescentam ingredientes interessantes no estudo da metodologia do controle ótimo linear feedback para sistemas não-lineares, na medida em que dois aspectos importantes do controle são abordados: tempo de sincronização e custo.

A possibilidade de relacionar esses dois aspectos do controle através do estudo da matriz Q foi explorada, e foi possível observar que tempo e custo podem ser reduzidos ao mesmo tempo, para determinados valores de Q . Assim, surgem novos horizontes quanto à escolha do critério Q para determinado sistema de controle pois, além de buscar a otimalidade do controle para um valor qualquer de um critério Q , ainda é possível selecionar o critério de forma a beneficiar a redução de tempo e custo de sincronização.

Como o estudo realizado no capítulo 5 agrega mais conhecimento a respeito do custo do controle ótimo linear feedback, surgem condições para que trabalhos futuros

estabeleçam comparações do custo do controle ótimo linear feedback com outros métodos de controle e sincronização de caos encontrados na literatura.

O capítulo 6 foi dedicado à introdução e teste do conceito de continuidade por partes na metodologia do controle linear feedback. Considerando a gama de situações onde não é possível ou desejável que a função de controle atue durante 100% do tempo de desempenho dos sistemas, a contribuição do estudo realizado no capítulo foi no sentido de abrir um novo horizonte para a aplicação do controle linear feedback na forma como proposto em [64].

Tendo em vista os resultados obtidos nas simulações numéricas conclui-se que, mesmo na forma contínua por partes e com seu tempo de atuação efetiva drasticamente reduzido, o controle linear feedback para sistemas não-lineares pode sincronizar assintoticamente sistemas caóticos.

É importante observar que sistemas caóticos amplificam exponencialmente quaisquer perturbações existentes. Assim, a sincronia assintótica dos sistemas caóticos de Lorenz com controle linear feedback contínuo por partes foi um resultado surpreendente e importante. Tendo em vista a natureza explorativa do estudo realizado, fica a expectativa de que futuros trabalhos ocupem-se de desenvolver aspectos da teoria subjacente à metodologia do controle linear feedback contínuo por partes.

O projeto do algoritmo de criptografia baseado em sincronização de caos levou em consideração diversas publicações especializadas nas áreas de sistemas caóticos, sincronização, e criptografia baseada em caos.

Como ponto de partida, o sistema caótico unificado foi minuciosamente estudado, bem como seus casos particulares, os sistemas de Lorenz, Chen e Lü. O interesse na utilização do sistema caótico unificado surgiu justamente pela riqueza de atratores que podem surgir pela variação de seu parâmetro α .

A seguir, diversas metodologias de sincronização de caos foram testadas. O controle linear feedback apresentou resultados superiores aos das metodologias de sincronização propostas e utilizadas em publicações como [13, 14, 25, 30, 35, 50], por dois motivos principais. O primeiro é a ampliação do intervalo do parâmetro α para o qual o sistema caótico unificado pode ser assintoticamente sincronizado, ou seja, de $\alpha \in [0, \frac{1}{11}]$ para a metodologia proposta em [50] para $\alpha \in [0, 1]$ para a metodologia utilizada neste

trabalho. Em segundo lugar, porque o controle ótimo linear feedback permite diminuir consideravelmente o tempo necessário para a sincronização dos sistemas transmissor/receptor, conforme mostram os resultados obtidos nos capítulos 3 e 4.

A respeito do algoritmo criptográfico proposto, destacamos que, consideradas as publicações especializadas dedicadas ao tema, o algoritmo proposto tem melhor desempenho do que os algoritmos que o antecederam [20, 34, 35, 40, 50, 60, 68]. Além disso, o algoritmo proposto oferece um nível de segurança satisfatório se levadas em consideração as formas de ataque conhecidas e publicadas até a presente data.

Em trabalhos futuros, estudos comparativos do custo de diferentes metodologias de controle em relação ao controle ótimo linear feedback podem ser exploradas. Como forma de complementar o estudo do algoritmo criptográfico, o problema da sincronização de caos pode ser abordado considerando-se a influência de ruído no resultado do processo de encriptação/decriptação.

REFERÊNCIAS

- [1] AGUIRRE, L.A.; TORRES, L.A.B. *Fixed point stability analysis of Chua's circuit: a case study with a real circuit*. Journal of Circuits, Systems and Computers, vol. 7, nr. 2. World Scientific Publishing Company, 1997.
- [2] ALLIGOOD, K.; SAUER, T.; YORKE, J.A. *Chaos: an introduction to dynamical systems*. Springer-Verlag New York, 1996.
- [3] ALVAREZ, G.; LI, S. *Breaking network security based on synchronized chaos*. Computer Communications, vol. 27, pág. 1679-1681, 2004.
- [4] ALVAREZ, G.; MONTOYA, F.; PASTOR, G.; ROMERA, M. *Cryptanalyzing na improved security modulated chaotic encryption scheme using cyphertext absolute value*. Chaos, Solitons & Fractals, vol. 23, março de 2005, pág. 1749-1756.
- [5] ALVAREZ, G.; LI, S. *Some basic requirements for chaos-based cryptosystems*. International Journal of Bifurcation and Chaos in Applied Sciences and Engineering, nr. 8, vol. 16, pág. 2129-2152, 2006.
- [6] ANDRIEVSKII, B.R.; FRADKOV, A.L. *Control of chaos: methods and applications*. Automation and Remote Control, vol. 64, nr. 5, 2003, pag.673-713.
- [7] BAKER, G.L.; GOLLUB, J.P. *Chaotic dynamics: an introduction*. New York: Cambridge University Press, 1996.
- [8] BERGÉ, P.; POMEAU, Y.; DUBOIS-GANCE, M. *Dos Ritmos ao caos*. São Paulo: Editora Unesp, 1995.
- [9] BOEIRA, J.P.; RAFIKOV, M. *Sincronização do sistema de Lotka-Volterra usando controle linear feedback*. Brazilian Conference on Dynamics, Control and Their Applications, Guaratinguetá, SP, Brasil, maio de 2005.
- [10] BOYCE, W.E.; DIPRIMA, R.C. *Elementary differential equations and boundary value problems*. New York: John Wiley and Sons Inc., 1992.
- [11] BRAUER, F.; NOHEL, J.A. *Qualitative theory of ordinary differential equations*. New York: WA Benjamin Inc, 1969.
- [12] BROWN, R.; KOCAREV, Ljupco. *A unifying definition of synchronization for dynamical systems*. Chaos, vol. 10, nr. 2, junho de 2000.

- [13] BRUCOLI, M.; CAFAGNA, D.; CARNIMEO, L. *Design of a hyperchaotic cryptosystem base don identical and generalized synchronization*. International Journal of Bifurcation and Chaos, vol. 9, nr 10, pág. 2027-2037, 1999.
- [14] BRUCOLI, M.; CAFAGNA, L.; CARNIMEO, L.; GRASSI, G. *Hyperchaotic circuits for secure communication: an efficient synchronization technique*. International Conference on Electronics, Circuits, and Systems, 1996. ICECS apos; 96., Proceedings of the Third IEEE, vol. 2, pág. 639-642, outubro de 1996.
- [15] BURNETT, Steve. *O guia oficial RSA*. Rio de Janeiro: Elsevier, 2002.
- [16] CHERRIER, E.; BOUTAYEB, M.; RAGOT, J. *Observer based synchronization and input recovery for a class of chaotic models*. *IEEE Transactions on Circuits and Systems - Part I* 53 (2006) 1977-1988.
- [17] CORRON, N.J. *A new approach to communications using chaotic signals*. IEEE Transactions on circuits and systems – I: fundamental theory and applications, vol 44, nr. 5, maio de 1997.
- [18] CRONIN, J. *Fixed points and topological degree in nonlinear analysis*. Providence: American Mathematical Society, 1964.
- [19] CROSS, Michael. *Introduction to Chaos: chapter 7 – Lyapunov exponents*. Disponível em www.cmp.caltech.edu/~mcc/Chaos_Course/Outline.html. Acessado em 14/05/2007.
- [20] CUOMO, K. M.; OPPENHEIM, A.V. *Circuit implementation of synchronized chaos with applications to communications*. Phys. Rev. Lett. 71, 65 - 68 (1993) [Issue 1 – July 1993]
- [21] DACHSELT, F.; KELBER, C.; SCHWARZ, W. *Chaotic coding and cryptoanalysis*. Technische Universität Dresden. Dresden, Germany, 1998.
- [22] ECKMANN, J. P.; RUELLE, D. *Ergodic theory of chaos and strange attractors*. Rev. Mod. Phys., 57(3):617, 1985.
- [23] EISENCRAFT, Márcio. *Sistemas de Comunicação Utilizando sinais Caóticos*. São Paulo: Escola Politécnica da Universidade de São Paulo, 2001.
- [24] ELABBASY, E.M.; AGIZA, H.N.; EL-DESSOKY, M.M. *Global chaos synchronization for four-scroll attractor by nonlinear control*. Scientific Research and Essay, vol. 1 (3), pag. 65-71, dezembro de 2006.

- [25] EMADZADEH, A.A.; HAERI, M. Global Synchronization of two different chaotic systems via nonlinear control. ICCAS 2005, KINTEX, Gyeonggi-Do, Korea.
- [26] FIEDLER-FERRARA, N.; PRADO, C.P.C. *Caos: uma introdução*. São Paulo: Editora Edgard Blücher Ltda, 1995.
- [27] GALIAS, Zbigniew. *Study of synchronization of linearly coupled hyperchaotic systems*. Proceedings of the European Conference on Circuit Theory and Design, ECCTD'97, vol. 1, 296-301, Budapeste, 1997.
- [28] GARFINKEL, Simon; SPAFFORD, Gene. *Practical Unix & internet security*. Sebastopol, CA - USA: O' Reilly & Associates Inc., 1996.
- [29] GLEICK, James. **Chaos Theory**. Disponível em <http://home.earthlink.net/~srrobin/chaosb.html>. Acessado em 15/09/2006.
- [30] GRASSI, G.; MASCOLO, S. *Design of nonlinear observers for hyperchaos synchronization using a scalar signal*. International Symposium on Circuits and Systems, 1998. ISCAS apos;98. Proceedings of the 1998 IEEE vol. 3, pág. 283-286, maio de 1998.
- [31] GRASSI, G.; MASCOLO, S. *Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal*. IEEE Transactions on Circuits and Systems I – Fundamental Theory and Applications, vol. 44, nr. 10, 1997.
- [32] GREBOGI, C.; OTT, E.; YORKE, J. *Controlling chaos*. Phys. Rev. Lett. 64, 2837 - 2837 (1990).
- [33] GRZYBOWSKI, J.M.V; RAFIKOV, M. *Synchronization of a unified chaotic system using optimal linear feedback control*. Brazilian Conference on Dynamics, Control and Their Applications, São José do Rio Preto, SP, Brasil, maio de 2007.
- [34] GRZYBOWSKI, J.M.V.; RAFIKOV, M. *Sincronização do sistema caótico unificado via controle ótimo linear feedback com aplicação em comunicação*. Procedimentos do XXX Congresso Nacional de Matemática Aplicada e Computacional, Florianópolis, SC, setembro de 2007.
- [35] HARB, A.M.; AHMAD, W.M. *Chaotic systems synchronization in secure communication systems*. Proceedings of the The 2006 World Congress in Computer Science Computer Engineering, and Applied Computing, Las Vegas, Nevada, USA, junho de 2006.
- [36] HWANG, C.C.; CHOW, H.Y.; WANG, Y.K. *A new feedback control of a modified Chua's circuit system*. Physica D 92 (1996), 95-100.

- [37] JIANG, G.P.; CHEN, G.; TANG, W.K.S. *A new criterion for chaos synchronization using linear state feedback control*. International Journal of Bifurcation and Chaos, vol. 13, nr. 5 (2003).
- [38] KAHN, David. *The Codebreakers*. New York: Scribner, 1996.
- [39] KIRK, Donald E. *Optimal control theory – an introduction*. New York: Dover Publications Inc., 2004.
- [40] KOCAREV, L.; PARLITZ, U. *General approach for chaotic synchronization with applications to communications*. Phys. Rev. Lett. vol. 74, nr. 25, junho de 1995.
- [41] KOCAREV, L.; PARLITZ, U.; BROWN, R. *Robust synchronization of chaotic systems*. Physical Review E, vol. 61, nr. 4, Abril, 2000.
- [42] KURTHS, J. *Control and synchronization in chaotic dynamical systems*. Chaos, vol. 13, nr. 1, março de 2003.
- [43] KWAKERNAAK, H.; SIVAN, R. *Linear optimal control systems*. New York: John Wiley and Sons, 1972.
- [44] LI, S.; LI, C.; CHEN, G.; MOU, X. *Cryptanalysis of the RCES/RSES image encryption scheme*. Elsevier Journal of Systems and Software at Apr. 2007, IACR's Cryptology ePrint Archive, Report 2004/376, 2004.
- [45] LI, D.; LU, J.; WU, X. *Linearly coupled synchronization of the unified chaotic systems and the Lorenz systems*. Chaos, Solitons & Fractals 23, 79-85, 2005.
- [46] LÜ, J.; CHEN, G.; CHENG, D. *A new chaotic system and beyond: the generalized Lorenz-like system*. International Journal of Bifurcation and Chaos, vol. 14, nr. 5 (2004), 1507-1537.
- [47] LU, J.; WU, X.; HAN, X.; LÜ, J. *Adaptive feedback synchronization of a unified chaotic system*. Physics Letters A 329 (2004), 327-333.
- [48] LÜ, J.; CHEN, G.; CHENG, D.; CELIKOVSKY, S. *Bridge the gap between the Lorenz system and the Chen system*. International Journal of Bifurcation and Chaos, vol. 12, nr. 12 (2002), 2917-2926, World Scientific Publishing Company.
- [49] LÜ, J.; CHEN, G.; ZHANG, S. *Controlling in between the Lorenz and Chen systems*. International Journal of Bifurcation and Chaos, vol. 12, nr. 6, 1417-1422, 2002.

- [50] LU, J.; WU, X.; LÜ, J. *Synchronization of a unified chaotic system and the application in secure communication*. Physics Letters A, nr. 305, 365-370, 2002.
- [51] MANCILLA, D.; HERNANDEZ, C. *A note on chaos-based communication schemes*. Revista Mexicana de Física 51 (3), 265-269, junho de 2005.
- [52] MASCOLO, S. *Backstepping design for controlling Lorenz chaos*. Procedures of the 36th CDC, San Diego, CA.
- [53] MIN, L.; JING, J. *A new theorem to synchronization of unified chaotic systems via adaptive control*. Journal of University of Science and Technology Beijing, vol. 10, nr. 6, pág. 72, dezembro de 2003.
- [54] MONTEIRO, Luiz Henrique Alves. *Sistemas Dinâmicos*. São Paulo: Ed. Livraria da Física, 2002.
- [55] NAIDU, D.S. *Optimal control systems*. Boca Ratón, FL: CRC Press, 2003.
- [56] NIJMEIJER, H. *A dynamical control view on synchronization*. Physica D 154 (2001), 219-228.
- [57] OKSASOGLU, A.; AKGUL, T. *Chaotic masking scheme with a linear inverse system*. Physical Review Letters, vol. 75, nr. 25, dezembro de 1995.
- [58] ORSINI, L.Q. *Introdução aos sistemas dinâmicos*. Rio de Janeiro: Guanabara Dois, 1985.
- [59] PECORA, L.M., et al. *Fundamentals of synchronization in chaotic systems, concepts and applications*. Chaos, vol. 7, nr. 4, 1997.
- [60] PECORA, L.; CARROLL, T. *Synchronization in chaotic systems*. Phys. Rev. Lett., vol. 64, nr. 8, pag. 821-824, 1990.
- [61] POGROMSKY, A.; NIJMEIJER, H. *Observer-based robust synchronization of dynamical systems*. International Journal of Bifurcation and Chaos, vol. 8, nr. 11, pág. 2243-2254, 1998.
- [62] PRIGOGINE, Ilya. *O fim das certezas*. São Paulo: Editora Unesp, 1996.
- [63] RAFIKOV, M.; BALTHAZAR, J.M. *On an optimal control design for Rössler system*. Physics Letters A 333 (2004) 241-245.

- [64] RAFIKOV M, BALTHAZAR J.M., *On control and synchronization in chaotic and hyperchaotic systems via linear feedback control*. Communications in Nonlinear Science and Numerical Simulation, 2007.
- [65] RAFIKOV, M.; BALTHAZAR, J.M. *Síntese do controle ótimo linear feedback para sistemas que exibem caos*. Anais do 3º Congresso Temático de Dinâmica e Controle da SBMAC, 2004.
- [66] *Routh Hurwitz Analysis*. Disponível em www.teicontrols.com/notes/AutomaticControlsEE362K/RouthHurwitzAnalysis.pdf. Acessado em 20/04/2007.
- [67] SINGH, Simon. *The Code Book*. New York: Dellacorte Press, 2001.
- [68] SOBHY, M.I.; SHEHATA, A.R. *Chaotic algorithm for data encryption*. International Conference on Acoustics, Speech, and Signal Processing, 2001. Proceedings, vol. 1, pág. i – xcii, 2001.
- [69] SOBHY, M. I.; SHEHATA, Alaa-eldin. *Methods of attacking chaotic encryption and countermeasures*. IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 2, pág. 1001–1004, 2001.
- [70] STEWART, Ian. *Será que Deus joga dados?* Rio de Janeiro: Jorge Zahar Ed., 1991.
- [71] STROGATZ, Steven H. *Sync: the emerging science of spontaneous order*. 1st Edition. New York: Hyperion Books, 2003.
- [72] TIAN, L.; XU, J.; SUN, M. *Chaos synchronization of the energy resource chaotic system with active control*. International Journal of Nonlinear Science, vol. 3, nr. 3, pág. 228-234, 2001.
- [73] TIGAN, Gheorghe. *Bifurcation and stability in a system derived from the Lorenz system*. Proceedings Of the 3-rd international colloquium of mathematics in engineering and numerical physics (menp-3).
- [74] VAIDYA, P.G.; ANAND, S. *Cryptography based on chaotic synchronization: round III*. (Prabhakar G Vaidya and Sajini Anand) (2005-06) <http://eprint.iacr.org/2005/273>.
- [75] WANG, C.; GE, S.S. *Adaptive backstepping control of uncertain Lorenz system*. International Journal of Bifurcation and Chaos, vol. 11, nr. 4, pág. 1115-1119, 2001.
- [76] WONG, K.W.; KWOK, B.S.H; LAW, W.S. *A fast image encryption scheme based on chaotic standard map*. Phys Lett A 2002; 298:238-42.

- [77] YANG, T.; YANG, C.M.; YANG, L.B.; *A detailed study of adaptive control of chaotic systems with unknown parameters*. Dynamics and Control, vol. 8, pág. 255-267, 1998.
- [78] YANG, T.. *A Survey of chaotic secure communication systems*. International Journal of Computational Cognition, vol. 2, nr. 2, pág. 81–130, junho de 2004.
- [79] YASSEN, M.T. *Chaos synchronization between two different chaotic systems using active control*. Chaos, Solitons and Fractals 23, pág. 131-140, 2005.
- [80] ZHONG, G.Q.; TANG. W.K.S. *Circuitry implementation and synchronization of Chen's attractor*. International Journal of Bifurcation and Chaos, vol. 12, nr. 6, pág. 1423-1427, 2002.

APÊNDICE A: CRITÉRIO DE ESTABILIDADE DE ROUTH-HURWITZ

Dada a equação característica de um sistema linear, o critério de estabilidade de Routh-Hurwitz permite determinar se existem raízes do polinômio que se localizam fora da metade esquerda do plano [56].

Seja a equação característica

$$f(s) = a_n s^n + a_{n-1} s^{n-1} + \dots + a_1 s + a_0 = 0$$

Duas condições necessárias mas não suficientes para que a equação característica tenha somente raízes com parte real negativa são:

- todos os coeficientes do polinômio devem ter o mesmo sinal;
- todos os coeficientes do polinômio devem ser diferentes de zero.

Considerando a tabela de *Routh-Hurwitz*

$$\begin{array}{c|cccc}
 s^n & a_n & a_{n-2} & a_{n-4} & a_{n-6} & \dots \\
 s^{n-1} & a_{n-1} & a_{n-3} & a_{n-5} & a_{n-7} & \dots \\
 s^{n-2} & b_1 & b_2 & b_3 & \dots & \\
 s^{n-3} & c_1 & c_2 & c_3 & \dots & \\
 s^{n-4} & \vdots & \vdots & \vdots & & \\
 \vdots & \vdots & \vdots & \vdots & & \\
 s^1 & & & & & \\
 s^0 & & & & &
 \end{array}$$

Onde $a_i, i = (1, 2, 3, \dots, n)$ são os coeficientes do polinômio, e

$$b_1 = \frac{-1}{a_{n-1}} \begin{vmatrix} a_n & a_{n-2} \\ a_{n-1} & a_{n-3} \end{vmatrix}, \quad b_2 = \frac{-1}{a_{n-1}} \begin{vmatrix} a_n & a_{n-4} \\ a_{n-1} & a_{n-5} \end{vmatrix}, \quad b_3 = \frac{-1}{a_{n-1}} \begin{vmatrix} a_n & a_{n-6} \\ a_{n-1} & a_{n-7} \end{vmatrix};$$

$$c_1 = \frac{-1}{b_1} \begin{vmatrix} a_{n-1} & a_{n-3} \\ b_1 & b_2 \end{vmatrix}, \quad c_2 = \frac{-1}{b_1} \begin{vmatrix} a_{n-1} & a_{n-5} \\ b_1 & b_3 \end{vmatrix},$$

a condição necessária para que todas as raízes do polinômio tenham parte real negativa é que todos os termos da primeira coluna ($a_n, a_{n-1}, b_1, c_1, \dots$) da matriz tenham o mesmo sinal.

O número de mudanças de sinal indica o número de raízes com parte real positiva.

APÊNDICE B: *SKEW TENT MAP*

De acordo com [19], o mapa caótico

$$F(x) = \begin{cases} \frac{x}{p}, & \text{se } 0 \leq x < p \\ \frac{(1-x)}{(1-p)}, & \text{se } p \leq x < 1 \end{cases}$$

com parâmetro de controle p possui comportamento caótico para qualquer valor de $p \in (0,1)$, $x_0 \in [0,1]$, com $x_0 \neq p_0$.

Livros Grátis

(<http://www.livrosgratis.com.br>)

Milhares de Livros para Download:

[Baixar livros de Administração](#)

[Baixar livros de Agronomia](#)

[Baixar livros de Arquitetura](#)

[Baixar livros de Artes](#)

[Baixar livros de Astronomia](#)

[Baixar livros de Biologia Geral](#)

[Baixar livros de Ciência da Computação](#)

[Baixar livros de Ciência da Informação](#)

[Baixar livros de Ciência Política](#)

[Baixar livros de Ciências da Saúde](#)

[Baixar livros de Comunicação](#)

[Baixar livros do Conselho Nacional de Educação - CNE](#)

[Baixar livros de Defesa civil](#)

[Baixar livros de Direito](#)

[Baixar livros de Direitos humanos](#)

[Baixar livros de Economia](#)

[Baixar livros de Economia Doméstica](#)

[Baixar livros de Educação](#)

[Baixar livros de Educação - Trânsito](#)

[Baixar livros de Educação Física](#)

[Baixar livros de Engenharia Aeroespacial](#)

[Baixar livros de Farmácia](#)

[Baixar livros de Filosofia](#)

[Baixar livros de Física](#)

[Baixar livros de Geociências](#)

[Baixar livros de Geografia](#)

[Baixar livros de História](#)

[Baixar livros de Línguas](#)

[Baixar livros de Literatura](#)
[Baixar livros de Literatura de Cordel](#)
[Baixar livros de Literatura Infantil](#)
[Baixar livros de Matemática](#)
[Baixar livros de Medicina](#)
[Baixar livros de Medicina Veterinária](#)
[Baixar livros de Meio Ambiente](#)
[Baixar livros de Meteorologia](#)
[Baixar Monografias e TCC](#)
[Baixar livros Multidisciplinar](#)
[Baixar livros de Música](#)
[Baixar livros de Psicologia](#)
[Baixar livros de Química](#)
[Baixar livros de Saúde Coletiva](#)
[Baixar livros de Serviço Social](#)
[Baixar livros de Sociologia](#)
[Baixar livros de Teologia](#)
[Baixar livros de Trabalho](#)
[Baixar livros de Turismo](#)